PREMIER
MINISTRE

Liberté
Égalité
Fraternité

ÉTUDE D'IMPACT

PROJET DE LOI
relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité

NOR : PRMD2412608L/Bleue-1

15 octobre 2024

TABLE DES MATIERES

INTRODUCTION GENERALE

1. TRANSPOSITION DE LA DIRECTIVE SUR LA RESILIENCE DES ENTITES CRITIQUES (REC) ET REFONTE DU DISPOSITIF DE LA SECURITE DES ACTIVITES D'IMPORTANCE VITALE (SAIV)

Contexte général

Les infrastructures critiques indispensables au fonctionnement de la Nation sont exposées aux risques naturels, sanitaires, technologiques, mais également aux menaces d'origine anthropique. La directive (UE) 2022/2557 du Parlement européen et du Conseil sur la résilience des entités critiques (REC), adoptée le 14 décembre 2022, constitue l'aboutissement d'une réflexion portée à l'échelle européenne sur la protection des infrastructures nécessaires au fonctionnement du marché intérieur, initiée en 2008 avec une première directive (Directive 2008/114/CE du Conseil du 8 décembre 2008 concernant le recensement et la désignation des infrastructures critiques européennes ainsi que l'évaluation de la nécessité d'améliorer leur protection). Elle tient compte des leçons tirées de la pandémie de COVID-19, notamment en termes de sensibilité des chaînes d'approvisionnement, mais également du durcissement du contexte géopolitique.

L'ambition de cette nouvelle directive est d'améliorer la fourniture, dans le marché intérieur européen, des services considérés comme essentiels au maintien de fonctions sociétales ou d'activités économiques vitales, en renforçant la résilience des entités considérées comme critiques par les Etats membres, dans onze secteurs d'activité : l'énergie, les transports, le secteur bancaire, les infrastructures des marchés financiers, la santé, l'eau potable, les eaux résiduaires, les infrastructures numériques, l'administration publique, l'espace ainsi que la production, la transformation et la distribution de denrées alimentaires. Elle vise ainsi, d'une part, à prévoir un standard de protection minimale à l'ensemble des infrastructures critiques de l'Union, dont peuvent dépendre les entités situées sur le territoire national, et, d'autre part, à assurer une concurrence plus loyale entre ces différents opérateurs à l'échelle de l'Union, désormais soumis à des règles communes.

Ainsi, la France met déjà en œuvre, depuis 2006, un dispositif d'identification des opérateurs, publics ou privés, considérés d'importance vitale, qui ont la charge de garantir leur propre protection : le dispositif de sécurité des activités d'importance vitale (SAIV).

Le présent projet de loi vise ainsi à transposer la directive REC par le prisme d'une révision de ce dispositif national, en conservant ses principes cardinaux, tout en y intégrant les obligations inédites prévues par la directive et l'extension de son champ d'application à de nouveaux secteurs. L'objectif principal du Gouvernement est donc de maintenir un niveau

élevé de protection des infrastructures critiques, déjà éprouvé et connu des acteurs concernés, adapté au contexte actuel.

Le dispositif actuel de sécurité des activités d'importance vitale (SAIV)

Sur les fondements de l'ancien dispositif de protection des points et réseaux sensibles datant de l'ordonnance de 1958, cette politique publique a été véritablement instaurée en 2006, à la suite des attentats de Madrid (2004) et de Londres (2005).

L'actuel dispositif de sécurité des activités d'importance vitale vise à assurer la protection physique et cyber d'opérateurs (publics ou privés) identifiés comme indispensables pour la continuité d'activité de la Nation – ou, de manière plus marginale, pouvant présenter un danger grave pour la population.

Ce dispositif est inscrit dans le code de la défense (articles L. 1332-1 à L. 1332-7) et compte aujourd'hui plus de 300 opérateurs, désignés d'importance vitale par l'Etat, dans 12 secteurs d'activité. Chaque secteur est supervisé par un ministère coordonnateur.

SECTEUR	MINISTRE COORDONNATEUR
Activités civiles de l'Etat (ACE)	Ministre de l'intérieur
Activités judiciaires	Ministre de la justice
Activités militaires de l'Etat (AME)	Ministre des armées
Alimentation	Ministre chargé de l'agriculture
Communications électroniques, audiovisuel et information	Ministre chargé des communications électroniques
Energie	Ministre chargé de l'énergie
Espace et recherche	Ministre chargé de la recherche (transfert en cours au ministre chargé de l'économie et des finances)
Finances	Ministre chargé de l'économie et des finances
Gestion de l'eau	Ministre chargé de l'écologie
Industrie	Ministre chargé de l'industrie
Santé	Ministre chargé de la santé
Transports	Ministre chargé des transports

Les opérateurs d'importance vitale (OIV) exercent leurs activités d'importance vitale sur près de 1500 points d'importance vitale (PIV) (usines, locaux d'une administration, data center, etc.), répartis sur l'ensemble du territoire national (métropole et outre-mer). La désignation

des PIV s'appuie sur la notion de non-substituabilité des activités. Leur identification est protégée par le secret de la défense nationale.

Une responsabilité partagée entre l'Etat et les opérateurs d'importance vitale

Désignés par l'Etat, les opérateurs d'importance vitale sont tenus de garantir à leurs frais la sécurité de leurs sites et de leurs systèmes d'information les plus critiques (points et systèmes d'information d'importance vitale) contre tout risque et toute menace, notamment à caractère terroriste. Les OIV exposent à travers un certain nombre de documents de planification (plan de sécurité opérateur, plan particulier de protection) les choix de sécurité qui leur permettent de répondre à cette obligation de résultat.

Ils procèdent notamment :

- à une identification des points d'importance vitale (PIV) : établissements, installations et ouvrages nécessaires à la réalisation des activités d'importance vitale ;
- à une analyse de l'ensemble des risques (naturels, technologiques, sanitaires, etc.) et des menaces (malveillance, terrorisme, cyber, etc.) pouvant affecter les activités et points d'importance vitale ;
- à la déclinaison et à l'application des mesures Vigipirate qui concernent leur activité ;
- à une démonstration de leur dispositif de sécurité et de gestion de crise ;
- au respect du principe de défense en profondeur au sein de chaque PIV ;
- à la rédaction d'un plan de continuité ou de reprise d'activité (PCA/PRA) et à l'identification des personnels clés ;
- à la désignation d'un délégué à la défense et à la sécurité (DDS), habilité au secret de la défense nationale et interlocuteur privilégié du ministère coordonnateur. Au niveau de chaque PIV, l'opérateur peut désigner un délégué local à la défense et à la sécurité (DLDS), interlocuteur privilégié de la préfecture de département ;
- à la protection des informations et supports classifiés (statut d'OIV ; liste des PIV ; documents de planification de sécurité).

Depuis 2013, le code de la défense impose également aux OIV des obligations similaires en termes de cybersécurité, notamment pour leurs « systèmes d'information d'importance vitale » (SIIV).

En contrepartie, l'Etat veille à la bonne application du dispositif, mais surtout accompagne et soutient les opérateurs d'importance vitale, à travers notamment :

- l'approbation des documents de planification de sécurité rédigés par l'opérateur ;
- les visites et inspections des PIV par les zones de défense et de sécurité (sauf pour les opérateurs du secteur des activités militaires de l'Etat) ;

- la possibilité pour l'Etat d'imposer des mesures administratives et des sanctions pénales à l'encontre des OIV qui ne respecteraient pas leurs obligations de protection physique ou cyber ;
- l'évaluation des risques et menaces (directives nationales de sécurité, postures Vigipirate) ;
- la planification par l'autorité préfectorale des mesures de vigilance, de protection et de réaction mises en œuvre par la force publique en cas d'attaque sur un PIV (planification des moyens et modalités d'intervention, à travers un plan de protection externe, pouvant faire l'objet d'exercices) ;
- un rôle de conseil des OIV dans l'organisation de leur politique de sécurité et de continuité d'activité (ministère coordonnateur), leur cybersécurité (ANSSI) ou la sécurité de leur(s) PIV (zones de défense et de sécurité, préfecture de département) ;
- la transmission à l'opérateur qui en fait la demande d'un avis sur la compatibilité du comportement d'une personne souhaitant accéder à un PIV (enquêtes administratives de sécurité) ;
- l'encadrement d'une formation complémentaire pour les agents privés de sécurité exerçant dans des sites sensibles.

<u>Une politique impliquant l'Etat à tous les niveaux</u>

Les acteurs de ce dispositif sont, au niveau central :

- le secrétariat de la défense et de la sécurité nationale (SGDSN) par délégation du Premier ministre : pilotage du dispositif, suivi et évolution règlementaire, coordination interministérielle. L'ANSSI supervise directement le volet cyber ;
- les ministères coordonnateurs à travers les services des hauts fonctionnaires de défense et de sécurité (SHFDS) : supervision de l'ensemble des opérateurs d'importance vitale de leur(s) secteur(s) d'activité ;
- le ministère de l'intérieur et des Outre-mer : responsable de l'application territoriale du dispositif ; l'autorité militaire assure un suivi à part des opérateurs du secteur des activités militaires de l'Etat ;
- les 300 opérateurs d'importance vitale (OIV) et en particulier leurs délégués à la défense et à la sécurité (directeurs sûreté, officiers de sécurité, etc.).

Le SGDSN préside la commission interministérielle de défense et de sécurité (CIDS) des secteurs d'activité d'importance vitale. Réunie deux fois par an, cette commission acte le suivi et l'évolution du dispositif (désignation de nouveaux OIV/PIV, approbation des PSO) et traite de tout sujet d'intérêt pour la SAIV.

Les acteurs de ce dispositif sont, au niveau territorial :

- les préfets de département (notamment leurs services interministériels de défense et de protection civile) : supervision de l'application des mesures de sécurité prévues dans les plans particuliers de protection des PIV civils ; planification des moyens et des modalités d'intervention de l'Etat (forces de sécurité intérieure, moyens de la sécurité civile, et le cas échéant forces armées) à travers les plans de protection externe ;
- les préfets de zones de défense et de sécurité : coordination, assistance et contrôle de la mise en œuvre du dispositif pour l'ensemble des PIV de la zone (notamment pour les visites et contrôles des PIV civils) ;
- les 1500 points d'importance vitale (PIV) et en particulier leurs délégués locaux à la défense et à la sécurité.

Les préfets de zones président les commissions zonales de défense et de sécurité (CZDS) des secteurs d'activités d'importance vitale.

La directive européenne sur la résilience des entités critiques

La publication de la directive (UE) 2022/2557 du Parlement européen et du Conseil sur la résilience des entités critiques (REC), adoptée le 14 décembre 2022, constitue l'aboutissement d'une réflexion européenne sur la protection des infrastructures critiques, initiée en 2008 avec une première directive limitée aux secteurs des transports et de l'énergie.

La directive (UE) 2022/2557 a été négociée sous présidence française de l'UE, par la Représentation française près l'Union européenne (RPUE) avec l'appui du SGDSN. Les travaux nationaux ont notamment veillé à ce qu'elle soit conforme avec la vision française.

Elle doit être transposée dans notre droit national d'ici le 17 octobre 2024.

Objectifs de la directive

Cette directive vise à améliorer la fourniture, dans le marché intérieur, de services essentiels au maintien de fonctions sociétales ou d'activités économiques vitales en renforçant la résilience des opérateurs (appelés entités) critiques qui fournissent de tels services.

La directive REC remplace et refond en profondeur la directive de 2008 :

- elle prévoit le passage d'une logique de protection physique d'infrastructures à une logique de résilience et de continuité d'activité ;
- elle vise les « entités critiques » nationales (c'est-à-dire. les opérateurs), et non plus seulement les infrastructures critiques européennes (c'est-à-dire celles dont l'arrêt ou la destruction aurait un impact sur au moins deux États membres) ;
- elle s'inscrit dans une politique de résilience globale et cohérente puisque les entités critiques seront également soumises aux obligations de cyber-résilience prévues par la directive NIS 2 ;

- elle élargit le nombre de secteurs concernés. Le champ d'application couvre désormais 11 secteurs, qui correspondent presque parfaitement aux secteurs actuels de la SAIV : énergie, transports, infrastructures bancaires, infrastructures de marché financier, santé, eau potable, assainissement, infrastructures digitales, administration publique (niveau central), espace, alimentation.

La directive permet d'offrir un socle minimal commun de résilience à tous les opérateurs de l'UE. Ces derniers ne sont aujourd'hui pas tous couverts par un dispositif comparable à celui mis en œuvre en France, ce qui rétablira une forme de concurrence loyale à l'échelle européenne.

La transposition de la directive européenne REC consolide le dispositif existant de sécurité des activités d'importance vitale (SAIV)

Pour éviter de créer un nouveau dispositif, la transposition repose sur une révision du dispositif national de sécurité des activités d'importance vitale défini dans le code de la défense (L. 1332-1 et suivants) et non sur une refonte de ses principes fondateurs ou la création d'un dispositif inédit. Cette politique publique a prouvé son efficacité et fait l'objet d'une déclinaison sur l'ensemble du territoire national.

Cette réforme normative et doctrinale constitue ainsi l'opportunité de moderniser notre dispositif national : rationalisation de la classification du dispositif (statut d'OIV, plan de continuité d'activité), simplification des documents de planification requis, ou encore renforcement des modalités de supervision, dans une logique de cohérence et d'efficacité.

La transposition s'inscrit dans une politique de résilience globale et cohérente. Les entités critiques seront également soumises aux obligations prévues par :

- 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 (NIS 2 – négociée en parallèle de la directive REC) ;
- la 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 (DORA).

C'est dans ce contexte qu'il a été décidé de construire un projet de loi commun « Résilience » pour la transposition de ces trois textes et pour prendre certaines dispositions pertinentes dans leurs champs respectifs.

Pour les autorités administratives compétentes, le renforcement du suivi du dispositif est nécessaire

Le vocabulaire national est conservé, de même que la logique d'identification des sites les plus sensibles (points d'importance vitale) ainsi que la planification associée, qui intégrera désormais les enjeux de résilience.

Le suivi effectué par le SGDSN, les ministères coordonnateurs, les zones de défense et de sécurité et les préfets de département est maintenu et pourra être renforcé.

En effet, la directive impose la révision des documents de planification (évaluation des risques, plan de résilience des opérateurs) tous les 4 ans. Cela demandera un suivi continu des services au niveau national et à l'échelle territoriale afin de renforcer la résilience de la Nation.

Pour les opérateurs d'importance vitale, une part importante des exigences de la directive sont déjà mises en œuvre à travers le dispositif actuel

Les entités concernées par la révision du dispositif SAIV sont les opérateurs qui étaient déjà désignés dans le dispositif existant, que ce soit au titre de l'activité d'importance vitale qu'ils opèrent ou du danger grave pour la population qu'ils pourraient causer en cas d'incident.

De nouveaux opérateurs d'importance vitale pourraient néanmoins être désignés au titre de leurs activités, considérées comme d'importance vitale par l'Etat si celles-ci devaient évoluer ou émerger, en particulier dans les secteurs de l'assainissement, de l'hydrogène, ainsi que les réseaux de chaleur et de froid, nouvellement identifiés par la directive REC.

Le nombre d'opérateurs d'importance vitale (environ 300 à ce jour) n'a donc pas vocation à augmenter significativement.

Concrètement, la mise en œuvre de la directive devrait se traduire par :

- une mise à jour de la planification, en conservant son architecture actuelle et en renforçant la composante « continuité d'activité » (déjà prévue dans le dispositif actuel au titre du L. 2151-1 du code de la défense) ;
- une meilleure prise en compte des interdépendances entre les secteurs (notamment infrastructures de réseaux), y compris entre Etats membres avec l'identification par les opérateurs de leurs interdépendances et de leurs chaînes d'approvisionnement ;
- une obligation de notification des incidents majeurs (suivant le principe qui existe déjà en matière cyber, avec des modalités d'application spécifiques) ;
- une évolution et un renforcement du dispositif d'enquêtes administratives de sécurité : extension aux demandes d'accès à distance et aux fonctions sensibles, consultation des casiers judiciaires des ressortissants des autres Etats membres de l'UE ;
- une révision du dispositif de sanctions pour les opérateurs qui ne respecteraient pas leurs obligations : substitution d'un régime de sanctions administratives au régime des sanctions

pénales existant. L'objectif est de s'aligner sur les dispositions prévues dans la directive NIS 2.

La création d'un nouveau statut, celui d'« entité critique d'importance européenne particulière » (ECIEP) pour les opérateurs fournissant un/des services essentiels à au moins 6 Etats membres de l'UE, porte des enjeux particuliers : obligation de notification à la Commission et de partage d'information avec les Etats membres concernés. Néanmoins, il convient de souligner que la directive REC a été négociée (et le SGDSN a été particulièrement vigilant sur ce point) dans l'objectif de respecter les prérogatives nationales et les enjeux de souveraineté, de sécurité, de protection du secret afférent à la protection des infrastructures critiques, de sorte que :

- l'identité des entités critiques nationales ne sera pas communiquée à la Commission ;
- l'Etat membre reste le seul interlocuteur des opérateurs ;
- seules les données agrégées seront transmises à la Commission.

L'essentiel des obligations s'appliqueront à l'ensemble des secteurs d'activité d'importance vitale, y compris ceux ne figurant pas dans le champ d'application de la directive REC, afin d'aligner vers le haut le niveau d'exigence imposé aux opérateurs, en particulier pour les opérateurs relevant des secteurs régaliens.

Les mesures de résilience prévues pourraient engendrer des coûts supplémentaires pour un opérateur. Si la logique de protection physique était déjà prise en compte, la systématisation de la prise en compte de la continuité d'activité ne sera en effet pas neutre, bien qu'elle soit déjà prévue par le code de la défense.

Pour autant, l'identification et la mise en œuvre de mesures préventives et réactives garantissant la résilience de l'opérateur lui permettront de maintenir son activité dans un contexte dégradé et contribuent à prévenir des coûts potentiellement bien supérieurs en cas de disruption de son activité. En outre, la résilience accrue de l'ensemble des opérateurs est également de nature à prévenir l'apparition de coûts en cas de disruption de l'activité d'un fournisseur pour les mêmes motifs.

Enfin, dans l'objectif d'offrir aux entités tous les moyens pour qu'ils puissent effectivement mettre en œuvre des mesures de protection adaptées de leurs sites, le choix a été fait d'autoriser les opérateurs publics à déroger, dans certains cas précis, aux règles de la commande publique.

<u>Pour les collectivités territoriales, l'objectif est une meilleure cohérence du dispositif</u>

Les collectivités concernées par la directive REC sont celles qui sont déjà désignées OIV car assurant des « activités d'importance vitale » – ou services essentiels au sens de la directive REC lorsque l'activité est dans le champ d'application de la directive – dans les secteurs qui

relèvent de leur compétence : par exemple pour les secteurs de la gestion de l'eau, des transports et de l'énergie.

Dans le cas d'une délégation de service public pour des activités d'importance vitale, le présent projet de loi prévoit l'information de la collectivité territoriale du statut d'opérateur d'importance vitale de son délégataire.

De nouvelles collectivités territoriales, dans un nombre limité, pourraient être désignées au titre de leurs compétences dans les secteurs de l'assainissement, de l'hydrogène, ainsi que les réseaux de chaleur et de froid.

2. TRANSPOSITION DE LA DIRECTIVE NIS 2 (*NETWORK AND INFORMATION SECURITY*) POUR AMELIORER LA SECURITE DES SYSTEMES D'INFORMATION DES ENTREPRISES ET DES ADMINISTRATIONS.

Le titre II, Cybersécurité, a principalement pour objet de transposer la directive (UE) 2022/2555 (dite directive NIS 2) 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.

Elle remplace 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 directive NIS1), laquelle a été transposée en France par 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. Afin de garantir la résilience des « activités essentielles pour l'économie et la société de l'Union européenne », la directive NIS1 avait établi les bases d'une cybersécurité renforcée sur un ensemble de secteurs d'activité sur le territoire de l'Union européenne. Depuis 2016, la menace cyber a fortement évolué, devenant systémique. Alors que les cyber-attaquants se concentraient jusqu'à il y a quelques années sur les acteurs et opérateurs stratégiques, ils ciblent désormais l'ensemble du tissu social et économique. Au-delà de la menace stratégique (étatique) qui perdure, les cybercriminels sont entrés dans une logique de vastes campagnes d'attaques qui affectent un nombre beaucoup plus élevé de victimes (PME, collectivités territoriales, hôpitaux, etc.), avec parfois des conséquences extrêmement dommageables pour nos concitoyens.

Ainsi, la France a porté au niveau européen, pendant sa présidence du Conseil de l'Union européenne, la négociation d'une réglementation ambitieuse, la directive NIS 2. Elle détermine des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union européenne pour certaines entités qualifiées comme essentielles ou importantes, en raison des services qu'elles fournissent et de leur taille.

Un « passage à l'échelle » pour répondre à la massification de la menace cyber

La directive NIS 2 directive élargit considérablement le périmètre des acteurs et secteurs régulés par NIS1. En France, cela se traduit par une augmentation du nombre d'entités régulées de 500 à 15 000 entités environ, et une augmentation du nombre de secteurs régulés de 6 à 18 secteurs[1]. Le périmètre retenu dans le projet de loi français cible précisément les secteurs et les types d'entités ayant le plus grand impact potentiel sur l'économie et la société françaises.

La directive élargit également le périmètre des systèmes d'information à sécuriser. Alors que NIS1 prévoyait une identification des systèmes d'information essentiels sur lesquels les obligations de la directive porteraient, la directive NIS 2 s'applique par défaut à l'ensemble des systèmes d'information de l'entité. Des mécanismes d'exemption de certains systèmes d'information seront toutefois permis si ces derniers n'affectent pas la réalisation des activités ou la fourniture des services de l'entité.

Simplification, harmonisation et proportionnalité des règles

La directive européenne NIS 2 consacre le principe de proportionnalité en prévoyant deux niveaux d'entités régulées, classées selon leur degré de criticité, leur taille et leur chiffre d'affaires (pour les entreprises) : les entités essentielles et les entités importantes. Cette distinction permet d'adapter le niveau d'exigence.

- Les entités importantes, qui représentent la plus grande proportion des acteurs concernés par le projet de loi, se verront imposer des exigences de sécurité de base (de l'ordre de « l'hygiène numérique »), qui doivent les aider à prendre conscience de l'enjeu cyber et de l'impact particulièrement dommageable que les cyberattaques pourraient avoir sur leurs activités. Le niveau d'exigence requis vis-à-vis de ces entités a été conçu pour diminuer leur probabilité d'être atteintes par un rançongiciel courant, sans nécessiter des investissements disproportionnés. Une certaine latitude leur sera laissée pour mettre en œuvre les recommandations de sécurité les plus adaptées à leur connaissance des impacts potentiels d'une attaque, à leur environnement éventuellement spécifique, ainsi qu'à leurs moyens.
- Les entités essentielles sont des structures déjà sensibilisées ou confrontées à la menace cyber. Elles seront en partie des opérateurs déjà régulés, et donc déjà soumises depuis des années à la réglementation NIS et/ou au dispositif de sécurité des activités d'importance

[1] La directive européenne NIS1 couvrait initialement les secteurs suivants : Eaux potables, Energie, Finances, Infrastructures Numériques, Santé, Transports. Lors de sa transposition au niveau français sont introduits les secteurs suivants : Assurance, Eaux non potables, Education, Emploi, Logistique, Restauration, Social. Dans le cadre de NIS 2, de nouveaux secteurs sont ajoutés : Services TIC (interentreprises), Administration publique (de l'Etat et du territoire), Espace, Services postaux et d'expédition, Gestion des déchets, Fabrication (dont produits chimiques), Recherche, Fournisseurs numériques, Agroalimentaire.

vitale (SAIV). Celles qui ne sont pas déjà régulées sont pour la plupart des entités dont les critères de taille et de chiffre d'affaires (hors entités de l'administration) les situent dans une catégorie pour laquelle la dépendance aux infrastructures numériques ne fait pas de doute. Ceci suppose que la compétence et les moyens relatifs à la cybersécurité fassent déjà partie de leur gestion stratégique des risques.

Le modèle de référentiel d'exigences s'appuie sur des « objectifs de sécurité » pour répondre à la menace cyber contre laquelle la directive européenne entend protéger les entités. La façon d'atteindre ces objectifs pourra être adaptée aux risques, aux enjeux et aux spécificités d'un secteur d'activité ou d'une entité. Elle sera affinée au regard des retours des consultations en cours. Ces objectifs sont organisés autour de quatre axes :

- les entités devront se doter d'une gouvernance par la conformité et les risques visant à s'assurer que le risque numérique est pris en compte au plus haut niveau de l'entité, comme peut l'être le risque juridique et financier par ailleurs ;
- les entités devront mettre en place des mesures de protection de leurs systèmes d'information afin de limiter l'occurrence d'un incident de sécurité ;
- les entités devront se doter de capacités de défense de leurs systèmes d'information afin de pouvoir réagir rapidement en cas de survenance d'un incident de sécurité pour en limiter les impacts ;
- les entités devront se doter de capacités de résilience afin de limiter les impacts liés à la survenance d'un incident de sécurité et de pouvoir revenir rapidement à une situation normale ;
- la directive NIS 2 renforce le régime de sanction qui s'appliquera aux entités régulées. Le mécanisme prévu pourra, selon les infractions, se fonder sur un pourcentage du chiffre d'affaires mondial de l'entité concernée, à l'image de ce qui est prévu dans le Règlement général sur la protection des données (RGPD) : 2 % pour les entités essentielles et 1,4 % pour les entités importantes.

Le régime de sanction établi par ce projet de loi vise avant tout un objectif dissuasif, en permettant de matérialiser le coût invisible des attaques – bien supérieur généralement aux seules sanctions – et d'aider les acteurs à prendre les bonnes décisions d'investissement.

De l'importance d'intégrer les collectivités territoriales dans cette réglementation

Les attaques informatiques affectant les collectivités territoriales sont nombreuses. De janvier 2022 à juin 2023, l'ANSSI a traité 187 incidents les concernant. Ces incidents représentent 17 % de l'ensemble des incidents traités par l'agence sur la période.

Les conséquences d'attaques informatiques peuvent être majeures à l'échelle d'une collectivité territoriale, et affecter de multiples champs de compétences et de nombreux citoyens.

Alors que l'imposition de règles aux collectivités territoriales est laissée au libre choix des Etats membres dans la directive NIS 2, la France, qui a porté cette nécessité lors des négociations européennes, a fait le choix de les intégrer dans ces nouvelles exigences, au regard de la multiplication des attaques affectant les services publics locaux et leur faible sécurisation. L'objectif est d'adopter une approche proportionnée, adaptée aux moyens et à la maturité des acteurs.

1489 entités, collectivités territoriales et groupements de collectivités territoriales (661), ainsi que certains organismes sous leur tutelle devraient être concernés au titre des entités essentielles :

- les régions métropolitaines ainsi que les régions et les « pays et territoires d'outre-mer » (22 entités) ;
- les départements métropolitains et d'outre-mer (97 entités) ;
- les métropoles, communautés urbaines et communautés d'agglomérations métropolitaines et d'outre-mer (263 entités) ;
- les communes de plus de 30 000 habitants métropolitaines et d'outre-mer (279 entités) ;
- les centres de gestion (104 entités) ;
- les services départementaux d'incendie et de secours ;
- les syndicats dont les activités s'inscrivent dans un des secteurs d'activité hautement critiques ou critiques et dont la population bénéficiaire est supérieure à 30 000 habitants.

Les 992 communautés de communes métropolitaines et d'outre-mer seront quant à elles concernées au titre des entités importantes.

La très grande majorité des communes (99% ont moins de 30 000 habitants) ne sont donc concernées que par leur intercommunalité de rattachement.

1. TRANSPOSITION DE LA DIRECTIVE DORA (*DIGITAL OPERATIONAL RESILIENCE ACT*) EN VUE D'AMELIORER LA RESILIENCE DU SYSTEME BANCAIRE ET FINANCIER

Au cours des dernières décennies, l'utilisation des TIC est devenue centrale dans la fourniture de services financiers, au point qu'elles ont désormais acquis une importance cruciale dans

l’exécution des fonctions quotidiennes typiques de toutes les entités financières. La numérisation couvre maintenant, par exemple, les paiements, qui ont évolué progressivement de méthodes reposant sur les espèces et le papier vers l’utilisation de solutions numériques, ainsi que la compensation et le règlement des opérations sur titres, le trading électronique et algorithmique, les opérations de prêt et de financement, le financement entre pairs, la notation de crédit, la gestion de créances et les opérations de post-marché. Le secteur des assurances a également été transformé par l’utilisation des TIC avec l’apparition des intermédiaires d’assurance offrant des services en ligne et fonctionnant avec les technologies du domaine de l’assurance ou la souscription d’assurance. L’ensemble du secteur financier a non seulement opéré une transition vers le numérique à grande échelle, mais la numérisation a également renforcé les interconnexions et les relations de dépendance au sein du secteur financier et avec les prestataires tiers d’infrastructures et de services.

L’Union doit traiter de manière adéquate et globale les risques numériques auxquels sont exposées toutes les entités financières et qui découlent d’un recours accru aux technologies de l’information et de la communication (TIC) dans le cadre de la fourniture et de la consommation de services financiers, ce qui contribuera à exploiter le potentiel que recèle la finance numérique en matière de stimulation de l’innovation et de promotion de la concurrence dans un environnement numérique sûr.

Ces dernières années, le risque lié aux TIC a attiré l’attention des décideurs politiques, des régulateurs et des organismes de normalisation internationaux, nationaux et de l’Union, dans un effort visant à renforcer la résilience numérique, à définir des normes et à coordonner le travail de réglementation ou de surveillance. Au niveau international, le Comité de Bâle sur le contrôle bancaire, le Comité sur les paiements et les infrastructures de marché, le Conseil de stabilité financière, l’Institut pour la stabilité financière, ainsi que le G7 et le G20 s’efforcent de fournir aux autorités compétentes et aux opérateurs de marché des diverses juridictions des outils leur permettant de renforcer la résilience de leurs systèmes financiers. Ces travaux ont également été motivés par la nécessité de tenir dûment compte du risque lié aux TIC dans le contexte d’un système financier mondial fortement interconnecté et de veiller à une plus grande cohérence des bonnes pratiques pertinentes.

Au niveau de l’Union, les exigences liées à la gestion du risque lié aux TIC auquel est exposé le secteur financier sont actuellement prévues par les directives 2009/65/CE(4), 2009/138/CE(5), 2011/61/UE(6), 2013/36/UE(7), 2014/59/UE(8), 2014/65/UE(9), (UE) 2015/2366(10)et (UE) 2016/2341(11) du Parlement européen et du Conseil précédemment transposées en droit national.

Ces exigences sont diverses et parfois incomplètes. Dans certains cas, le risque lié aux TIC n’est abordé qu’implicitement dans le cadre du risque opérationnel et, dans d’autres cas, il n’est tout simplement pas abordé. Il est remédié à ces problèmes par l’adoption du règlement DORA (UE) 2022/2554 du Parlement européen et du Conseil entré en vigueur le 16 janvier 2023 et qui s'appliquera à partir du 17 janvier 2025. Il y a donc lieu de modifier ces directives

afin d'assurer la cohérence avec ledit règlement. La directive accompagnant le règlement DORA prévoit donc une série de modifications visant à garantir la clarté et la cohérence juridiques concernant l'application, par les entités financières agréées et soumises à une surveillance conformément auxdites directives, des diverses exigences en matière de résilience opérationnelle numérique nécessaires à l'exercice de leurs activités et à la prestation de services, assurant ainsi le bon fonctionnement du marché intérieur. Il est nécessaire de veiller à ce que ces exigences soient en adéquation avec les évolutions du marché, tout en encourageant la proportionnalité au regard notamment de la taille des entités financières et des régimes spécifiques auxquels elles sont soumises, en vue de réduire les coûts de mise en conformité.

Pour assurer une mise en œuvre cohérente du nouveau cadre en matière de résilience opérationnelle numérique du secteur financier, La France, ainsi que les autres États membres, doivent appliquer les disposition en droit national transposant la directive accompagnant le règlement DORA (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 transposition de la directive accompagnant DORA entraîne donc des modifications d'ordre technique au niveau national :

- du code monétaire et financier (article L. 314-1 ; article L. 420-3 ; article L. 421-11 ; article L. 511-41-1-B ; article L. 511-55 ; article L. 521-9 ; article L. 521-10 ; article L. 533-2 ; article L. 533-10 ; article L. 533-10-4 ; article L. 612-24 ; L. 613-38 ; article L. 631-1 ; articles L. 712-7, L. 761-1, L. 771-1, L. 781-1, L. 752-10, L. 753-10, L. 754-8, L. 762-3, L. 763-3, L. 764-3, L. 762-4, L. 763-4, L. 764-4, 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 et L. 785-3, L. 783-13, L. 784-13 et L. 785-12) ;
- du code de la mutualité (article L. 211-12 ; article L. 212-1) ;
- du code des assurances (article L. 354-1 ; article L. 356-18)
- et du code de la sécurité sociale (article L. 931-7).

Ces modifications techniques visent principalement à introduire des références croisées spécifiques au règlement DORA. L'objectif est de garantir une prise en compte adéquate du risque lié à l'utilisation des TIC dans le secteur financier et d'assurer ainsi une cohérence avec le règlement DORA.

Pour assurer une mise en œuvre cohérente du nouveau cadre en matière de résilience opérationnelle numérique du secteur financier, la France et les États membres doivent appliquer les dispositions de droit national transposant la directive accompagnant le règlement DORA avant le 17 janvier 2025, date d'application de ce dernier.

TABLEAU SYNOPTIQUE DES CONSULTATIONS

Article	Objet de l'article	Consultations obligatoires	Consultations facultatives
1er	Modifications du code de la défense	Conseil national d'évaluation des normes (CNEN)	Service National des Enquêtes Administratives de Sécurité Coordinateur général de la sécurité nucléaire Service juridique du Secrétariat Général des Affaires Européennes Agence Nationale de Sécurité des Systèmes d'Informations
2	Autres modifications du code de la défense, du code des postes et des communications électroniques, du code pénal, du code de la sécurité intérieure, du code de la santé publique et de la loi n° 2006-961 du 1er août 2006 relative au droit d'auteur et aux droits voisins dans la société de l'information	Conseil national d'évaluation des normes (CNEN)	Néant
3	Application en outre-mer	Conseil national d'évaluation des normes (CNEN)	Néant
4	Dispositions transitoires	Conseil national d'évaluation des normes (CNEN)	Néant
5	Missions et compétences de l'autorité nationale	Conseil national d'évaluation des normes (CNEN)	Commission nationale de l'informatique et des libertés (CNIL)
6	Définitions	Conseil national	Commission nationale de

		d'évaluation des normes (CNEN)	l'informatique et des libertés (CNIL)
7	Liste des secteurs d'activité hautement critiques et critiques	Conseil national d'évaluation des normes (CNEN) Commission supérieure du numérique et des postes (CSNP)	Prestataires qualifiés, associations professionnelles représentatives Commission nationale de l'informatique et des libertés (CNIL)
8	Critères d'identification des entités essentielles + Modalités de rétrogradation en entités importante ou d'exclusion du champ d'application de certaines administrations	Conseil national d'évaluation des normes (CNEN) Commission supérieure du numérique et des postes (CSNP)	Prestataires qualifiés, associations professionnelles représentatives Commission nationale de l'informatique et des libertés (CNIL)
9	Critères d'identification des entités importantes + Modalités d'exclusion du champ d'application de certaines administrations	Conseil national d'évaluation des normes (CNEN) Commission supérieure du numérique et des postes (CSNP)	Prestataires qualifiés, associations professionnelles représentatives Commission nationale de l'informatique et des libertés (CNIL)
10	Mécanismes et modalités de désignation unitaire d'entités importantes ou essentielles	Conseil national d'évaluation des normes (CNEN) Commission supérieure du numérique et des postes (CSNP)	Prestataires qualifiés, associations professionnelles représentatives Commission nationale de l'informatique et des libertés (CNIL)
11	Territorialité de l'application de la présente loi aux entités	Conseil national d'évaluation des normes (CNEN) Commission supérieure du numérique et des postes (CSNP)	Prestataires qualifiés, associations professionnelles représentatives Commission nationale de l'informatique et des libertés (CNIL)

12	Remontée d'informations des entités importantes et essentielles en vue de constituer la liste que la France devra communiquer à la Commission européenne	Conseil national d'évaluation des normes (CNEN) Commission supérieure du numérique et des postes (CSNP)	Prestataires qualifiés, associations professionnelles représentatives Commission nationale de l'informatique et des libertés (CNIL)
13	Dispositions particulières concernant les actes juridiques sectoriels européen qui pourraient s'appliquer en lieu et place de la transposition de NIS2	Conseil national d'évaluation des normes (CNEN) Commission supérieure du numérique et des postes (CSNP)	Prestataires qualifiés, associations professionnelles représentatives Commission nationale de l'informatique et des libertés (CNIL)
14	Application des mesures de sécurité aux entités importantes et essentielles et également les administrations « régaliennes », les juridictions administratives et judiciaires	Conseil national d'évaluation des normes (CNEN) Commission supérieure du numérique et des postes (CSNP)	Prestataires qualifiés, associations professionnelles représentatives Commission nationale de l'informatique et des libertés (CNIL)
15	Mécanismes permettant à une entité importante ou essentielle de se prévaloir de la conformité à un référentiel établi par l'autorité nationale pour démontrer sa conformité aux exigences prévues à l'article 14	Conseil national d'évaluation des normes (CNEN) Commission supérieure du numérique et des postes (CSNP)	Prestataires qualifiés, associations professionnelles représentatives Commission nationale de l'informatique et des libertés (CNIL)
16	Exigences particulières relatives au volet cyber du dispositif de sécurité des activités d'importance vitale et aux systèmes d'information de l'administration supportant des échanges par voie électronique avec leurs usagers ou d'autres administrations	Conseil national d'évaluation des normes (CNEN) Commission supérieure du numérique et des postes (CSNP)	Prestataires qualifiés, associations professionnelles représentatives Commission nationale de l'informatique et des libertés (CNIL)
17	Notifications d'incidents et	Conseil national d'évaluation des normes	CSIRT ministériels, sectoriels et territoriaux,

	vulnérabilités importants	(CNEN) Commission supérieure du numérique et des postes (CSNP)	prestataires qualifiés Commission nationale de l'informatique et des libertés (CNIL)
18	Champ d'application organique de la section relative à l'enregistrement des noms de domaine	Conseil national d'évaluation des normes (CNEN) Autorité de régulation des communications électroniques, des postes et de la distribution de la presse (ARCEP) Commission supérieure du numérique et des postes (CSNP)	Commission nationale de l'informatique et des libertés (CNIL)
19	Collecte des données nécessaires à l'enregistrement des noms de domaine	Conseil national d'évaluation des normes (CNEN) Commission supérieure du numérique et des postes (CSNP) Autorité de régulation des communications électroniques, des postes et de la distribution de la presse (ARCEP)	Commission nationale de l'informatique et des libertés (CNIL)
20	Conservation des données liées à l'enregistrement des noms de domaine	Conseil national d'évaluation des normes (CNEN) Autorité de régulation des communications électroniques, des postes et de la distribution de la presse (ARCEP) Commission supérieure du numérique et des postes (CSNP)	Commission nationale de l'informatique et des libertés (CNIL)

21	Publication des données liées à l'enregistrement des noms de domaine	Conseil national d'évaluation des normes (CNEN) Autorité de régulation des communications électroniques, des postes et de la distribution de la presse (ARCEP) Commission supérieure du numérique et des postes (CSNP)	Commission nationale de l'informatique et des libertés (CNIL)
22	Règles d'accès par les agents habilités par l'autorité judiciaire ou par l'autorité nationale de sécurité des systèmes d'information des données liées à l'enregistrement des noms de domaine	Conseil national d'évaluation des normes (CNEN) Autorité de régulation des communications électroniques, des postes et de la distribution de la presse (ARCEP) Commission supérieure du numérique et des postes (CSNP)	Commission nationale de l'informatique et des libertés (CNIL)
23	Partage d'informations nécessaires à l'accomplissement de leurs missions respectives entre l'Autorité nationale de sécurité des systèmes d'information d'une part et certains organismes d'autre part (par exemple, la CNIL ou autorité compétente au regard d'un acte juridique sectoriel)	Conseil national d'évaluation des normes (CNEN) Commission supérieure du numérique et des postes (CSNP)	Commission nationale de l'informatique et des libertés (CNIL) CSIRT ministériels, sectoriels et territoriaux, prestataires qualifiés
24	Agrément pour les relais de prévention et de gestion des incidents	Conseil national d'évaluation des normes (CNEN) Commission supérieure du numérique et des postes (CSNP)	Commission nationale de l'informatique et des libertés (CNIL) CSIRT ministériels, sectoriels et territoriaux, prestataires qualifiés
25	Supervision	Conseil national	Commission nationale de

		d’évaluation des normes (CNEN) Commission supérieure du numérique et des postes (CSNP)	l’informatique et des libertés (CNIL)
26	Habilitation des agents amenés à rechercher et constater des manquements, notamment aux dispositions de la présente loi	Conseil national d’évaluation des normes (CNEN) Commission supérieure du numérique et des postes (CSNP)	Commission nationale de l’informatique et des libertés (CNIL)
27	Nature des activités de contrôle	Conseil national d’évaluation des normes (CNEN) Commission supérieure du numérique et des postes (CSNP)	Commission nationale de l’informatique et des libertés (CNIL)
28	Coopération de la personne contrôlée et amende en cas d’obstacle à un contrôle	Conseil national d’évaluation des normes (CNEN) Commission supérieure du numérique et des postes (CSNP)	Commission nationale de l’informatique et des libertés (CNIL)
29	Nature des activités de contrôle	Conseil national d’évaluation des normes (CNEN) Commission supérieure du numérique et des postes (CSNP)	Commission nationale de l’informatique et des libertés (CNIL)
30	Modalités d’application de la sous-section 2 de la section 1 du chapitre III (art. 27 à 29)	Conseil national d’évaluation des normes (CNEN) Commission supérieure du numérique et des postes (CSNP)	Commission nationale de l’informatique et des libertés (CNIL)
31	Ouverture de la procédure à l’encontre de la personne	Conseil national d’évaluation des normes	Commission nationale de l’informatique et des

	contrôlée	(CNEN) Commission supérieure du numérique et des postes (CSNP)	libertés (CNIL)
32	Mesure d'exécution	Conseil national d'évaluation des normes (CNEN) Commission supérieure du numérique et des postes (CSNP)	Commission nationale de l'informatique et des libertés (CNIL)
33	Notification des griefs et saisine de la commission des sanctions	Conseil national d'évaluation des normes (CNEN) Commission supérieure du numérique et des postes (CSNP)	Commission nationale de l'informatique et des libertés (CNIL)
34	Modalités d'application de la section 2 du chapitre III (art. 31 à 33)	Conseil national d'évaluation des normes (CNEN) Commission supérieure du numérique et des postes (CSNP)	Commission nationale de l'informatique et des libertés (CNIL)
35	Commission des sanctions	Conseil national d'évaluation des normes (CNEN) Commission supérieure du numérique et des postes (CSNP)	Commission nationale de l'informatique et des libertés (CNIL) CSIRT ministériels, sectoriels et territoriaux, prestataires qualifiés
36	Composition de la commission des sanctions	Conseil national d'évaluation des normes (CNEN) Commission supérieure du numérique et des postes (CSNP)	Commission nationale de l'informatique et des libertés (CNIL) CSIRT ministériels, sectoriels et territoriaux, prestataires qualifiés
37	Nature de sanction	Conseil national d'évaluation des normes (CNEN)	Commission nationale de l'informatique et des libertés (CNIL)

		Commission supérieure du numérique et des postes (CSNP)	CSIRT ministériels, sectoriels et territoriaux, prestataires qualifiés
38	Alléger le contrôle des biens de cryptologie	Conseil national d'évaluation des normes (CNEN)	Acteurs industriels Commission nationale de l'informatique et des libertés (CNIL)
39	Modification de l'ordonnance n° 2005-1516 du 8 décembre 2005, de la loi n° 2018-133 du 3 février 2018, de certaines dispositions du code de la défense et de certaines dispositions du code des postes et des communications électroniques	Conseil national d'évaluation des normes (CNEN) Autorité de Régulation des Communications Electroniques, des Postes et de la distribution de la Presse (ARCEP)	Commission nationale de l'informatique et des libertés (CNIL)
40	Mesures applicables à l'outre-mer pour les territoires sous spécialité législative	Conseil national d'évaluation des normes (CNEN)	Commission nationale de l'informatique et des libertés (CNIL)
41	Renforcement des sanctions pénales pour améliorer la lutte contre les brouillages	Conseil national d'évaluation des normes (CNEN) Autorité de Régulation des Communications Electroniques, des Postes et de la distribution de la Presse (ARCEP)	Commission nationale informatique et des libertés (CNIL)
42	Renforcement des conditions d'accès à une assignation de fréquences déposées par la France auprès de l'Union Internationale des Télécommunications	Conseil national d'évaluation des normes (CNEN) Autorité de Régulation des Communications Electroniques, des Postes et de la distribution de la Presse (ARCEP)	Commission nationale informatique et des libertés (CNIL) Commission supérieure du numérique et des postes (CSNP)
43	Modification de la définition des prestataires de services techniques	Comité consultatif de la législation et de la	Autorité de contrôle prudentiel et de résolution

		réglementation financières (CCLRF)	(ACPR)
44	Maintien de la résilience opérationnelle des gestionnaires de plateformes de négociation	Comité consultatif de la législation et de la réglementation financières (CCLRF)	Autorité des marchés financiers (AMF)
45	Gestion du risque lié aux technologies de l'information et de la communication par les entreprises de marché	Comité consultatif de la législation et de la réglementation financières (CCLRF)	Autorité des marchés financiers (AMF)
46	Référence 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	Comité consultatif de la législation et de la réglementation financières (CCLRF)	Autorité de contrôle prudentiel et de résolution (ACPR) Association française des Sociétés Financières (ASF)
47	Référence aux réseaux et systèmes d'information au sein des exigences de contrôle interne des établissements de crédit et des sociétés de financement	Comité consultatif de la législation et de la réglementation financières (CCLRF)	Autorité de contrôle prudentiel et de résolution (ACPR) Association française des Sociétés Financières (ASF)
48	Obligations des prestataires de services de paiement en matière de gestion du risque lié aux technologies de l'information et des communications (TIC)	Comité consultatif de la législation et de la réglementation financières (CCLRF)	Autorité de contrôle prudentiel et de résolution (ACPR)
49	Modification de la liste des prestataires de services de paiement soumis à une obligation de notification des incidents opérationnels ou de sécurité majeur	Comité consultatif de la législation et de la réglementation financières (CCLRF)	Autorité de contrôle prudentiel et de résolution (ACPR)
50	Référence aux réseaux et systèmes d'information au sein des exigences de contrôle et de sauvegarde des prestataires de service d'investissement	Comité consultatif de la législation et de la réglementation financières (CCLRF)	Autorité de contrôle prudentiel et de résolution (ACPR) Association française des

			Sociétés Financières (ASF)
51	Systèmes de technologies de l'information et de la communication (TIC) et dispositifs de contrôle des prestataires de services d'investissement	Comité consultatif de la législation et de la réglementation financières (CCLRF)	Autorité des marchés financiers (AMF)
52	Systèmes de contrôle des risques mis en œuvre par les prestataires de services d'investissement autres que les sociétés de gestion de portefeuille qui ont recours à la négociation algorithmique	Comité consultatif de la législation et de la réglementation financières (CCLRF)	Autorité des marchés financiers (AMF)
53	Référence aux prestataires informatiques critiques au sein des tiers auxquels l'Autorité de contrôle prudentiel et de résolution peut demander toute information	Comité consultatif de la législation et de la réglementation financières (CCLRF)	Autorité de contrôle prudentiel et de résolution (ACPR) Association française des Sociétés Financières (ASF)
54	Référence à la résilience opérationnelle numérique au sein des plans préventifs de résolution des établissements de crédit et des sociétés de financement	Comité consultatif de la législation et de la réglementation financières (CCLRF)	Autorité de contrôle prudentiel et de résolution (ACPR) Association française des Sociétés Financières (ASF)
55	Extension de la liste des autorités habilitées à s'échanger des informations	Comité consultatif de la législation et de la réglementation financières (CCLRF)	Autorité de contrôle prudentiel et de résolution (ACPR)
56	Modification du code monétaire et financier	Comité consultatif de la législation et de la réglementation financières (CCLRF)	
57	Nouvelles obligations pour les entreprises d'assurance et de réassurance en matière de gouvernance des risques liés à l'utilisation des systèmes	Comité consultatif de la législation et de la réglementation financières (CCLRF)	Autorité de contrôle prudentiel et de résolution (ACPR) Association France

	d'information		Assureurs Centre technique des institutions de prévoyance (CTIP) Fédération nationale de la Mutualité française (FNMF)
58	Extension aux groupes d'assurance des nouvelles obligations de gouvernance des risques liés à l'utilisation des systèmes d'information	Comité consultatif de la législation et de la réglementation financières (CCLRF)	Autorité de contrôle prudentiel et de résolution (ACPR) Association France Assureurs Centre technique des institutions de prévoyance (CTIP) Fédération nationale de la Mutualité française (FNMF)
59	Nouvelles obligations pour les unions et mutuelles du code de la mutualité en matière de gouvernance des risques liés à l'utilisation des systèmes d'information	Comité consultatif de la législation et de la réglementation financières (CCLRF)	Autorité de contrôle prudentiel et de résolution (ACPR) Association France Assureurs Centre technique des institutions de prévoyance (CTIP) Fédération nationale de la Mutualité française (FNMF)
60	Suppression de dispositions redondantes dans le code de la mutualité	Comité consultatif de la législation et de la réglementation financières (CCLRF)	Autorité de contrôle prudentiel et de résolution (ACPR) Association France Assureurs Centre technique des institutions de prévoyance (CTIP) Fédération nationale de la Mutualité française (FNMF)
61	Nouvelles obligations pour les institutions de prévoyance et	Comité consultatif de la législation et de la	Autorité de contrôle prudentiel et de résolution

	unions du code de la sécurité sociale en matière de gouvernance des risques liés à l'utilisation des systèmes d'information	réglementation financières (CCLRF)	(ACPR) Association France Assureurs Centre technique des institutions de prévoyance (CTIP) Fédération nationale de la Mutualité française (FNMF)
62	Dates d'application des dispositions du titre III sur la résilience opérationnelle numérique du secteur financier	Comité consultatif de la législation et de la réglementation financières (CCLRF)	Autorité de contrôle prudentiel et de résolution (ACPR) Association française des Sociétés Financières (ASF)

TABLEAU SYNOPTIQUE DES MESURES D'APPLICATION

Article	Objet de l'article	Textes d'application	Administration compétente
1er	Création de l'article L. 1332-1 du code de la défense Définitions	Néant	Sans objet
1er	Création de l'article L. 1332-2 du code de la défense Désignation des opérateurs d'importance vitale	Décret en Conseil d'Etat	Secrétariat général de la défense et de la sécurité nationale (SGDSN)
1er	Création de l'article L. 1332-3 du code de la défense Obligations de résilience	Décret en Conseil d'Etat	Secrétariat général de la défense et de la sécurité nationale (SGDSN)
1er	Création de l'article L. 1332-4 du code de la défense Analyse des dépendances	Décret en Conseil d'Etat	Secrétariat général de la défense et de la sécurité nationale (SGDSN)
1er	Création de l'article L. 1332-5 du code de la défense Mesures relatives aux points d'importance vitale (PIV) et plans particuliers de résilience (PPR)	Décret en Conseil d'Etat	Secrétariat général de la défense et de la sécurité nationale (SGDSN)
1er	Création de l'article L. 1332-6 du code de la défense Enquêtes administratives de sécurité	Décret en Conseil d'Etat	Secrétariat général de la défense et de la sécurité nationale (SGDSN)
1er	Création de l'article L. 1332-7 du code de la défense	Décret en Conseil d'Etat	Secrétariat général de la défense et de la sécurité

Article	Objet de l'article	Textes d'application	Administration compétente
	Notification d'incidents		nationale (SGDSN)
1er	Création de l'article L. 1332-8 du code de la défense Mission de conseil de la Commission européenne	Décret en Conseil d'Etat	Secrétariat général de la défense et de la sécurité nationale (SGDSN)
1er	Création de l'article L. 1332-9 du code de la défense Obligation des entités critiques d'importance européenne particulière	Décret en Conseil d'Etat	Secrétariat général de la défense et de la sécurité nationale (SGDSN)
1er	Création de l'article L. 1332-10 du code de la défense Protection des installations d'importance vitale	Néant	Sans objet
1er	Création de l'article L. 1332-11 du code de la défense Sécurisation des systèmes d'informations des opérateurs	Décret en Conseil d'Etat	Secrétariat général de la défense et de la sécurité nationale (SGDSN) Agence nationale de sécurité des systèmes d'informations (ANSSI)
1er	Création de l'article L. 1332-12 du code de la défense Désignation des agents chargés de la supervision et des contrôles des OIV / entités critiques	Décret en Conseil d'Etat	Secrétariat général de la défense et de la sécurité nationale (SGDSN)
1er	Création de l'article L. 1332-13 du code de la défense Devoirs et pouvoirs des agents chargés de la supervision des OIV / entités critiques	Décret en Conseil d'Etat	Secrétariat général de la défense et de la sécurité nationale (SGDSN)
1er	Création de l'article L. 1332-14 du code de la défense Interdiction de faire obstacle à un	Décret en Conseil d'Etat	Secrétariat général de la défense et de la sécurité nationale (SGDSN)

Article	Objet de l'article	Textes d'application	Administration compétente
	contrôle		
1er	Création de l'article L. 1332-15 du code de la défense Création de la commission des sanctions	Décret en Conseil d'Etat	Secrétariat général de la défense et de la sécurité nationale (SGDSN)
1er	Création de l'article L. 1332-16 du code de la défense Composition de la commission des sanctions	Décret en Conseil d'Etat	Secrétariat général de la défense et de la sécurité nationale (SGDSN)
1er	Création de l'article L. 1332-17 du code de la défense Sanctions pouvant être infligées par la commission des sanctions	Décret en Conseil d'Etat	Secrétariat général de la défense et de la sécurité nationale (SGDSN)
1er	Création de l'article L. 1332-18 du code de la défense Suites données aux sanctions	Décret en Conseil d'Etat	Secrétariat général de la défense et de la sécurité nationale (SGDSN)
1er	Création de l'article L. 1332-19 du code de la défense Modalités d'application de la sous-section	Décret en Conseil d'Etat	Secrétariat général de la défense et de la sécurité nationale (SGDSN)
1er	Création de l'article L. 1332-20 du code de la défense Marchés publics des opérateurs d'importance vitale	Décret en Conseil d'Etat	Secrétariat général de la défense et de la sécurité nationale (SGDSN)
1er	Création de l'article L. 1332-21 du code de la défense Contrats de concession des opérateurs d'importance vitale	Décret en Conseil d'Etat	Secrétariat général de la défense et de la sécurité nationale (SGDSN)
1er	Création de l'article L. 1332-22		Secrétariat général de la

Article	Objet de l'article	Textes d'application	Administration compétente
	du code de la défense Information de l'utilisation des dispositions des articles L. 1332-20 et L. 1332-21	Décret en Conseil d'Etat	défense et de la sécurité nationale (SGDSN)
2	Autres modifications du code de la défense, du code des postes et des communications électroniques, du code pénal, du code de la sécurité intérieure, du code de la santé publique et de la loi n° 2006-961 du 1er août 2006 relative au droit d'auteur et aux droits voisins dans la société de l'information	Néant	Sans objet
3	Application outre-mer	Néant	Sans objet
4	Dispositions transitoires	Néant	Sans objet
5	Missions et compétences de l'autorité nationale	Décret en Conseil d'Etat	Secrétariat général de la défense et de la sécurité nationale (SGDSN) / Agence nationale de sécurité des systèmes d'informations (ANSSI)
6	Définitions	Néant	Sans objet
7	Liste des secteurs d'activité hautement critiques et critiques	Décret en Conseil d'Etat	Secrétariat général de la défense et de la sécurité nationale (SGDSN) / Agence nationale de sécurité des systèmes d'informations (ANSSI)
8	Critères d'identification des entités essentielles + Modalités de rétrogradation en entités importante ou d'exclusion	Décret en Conseil d'Etat Arrêté	Agence nationale de sécurité des systèmes d'informations (ANSSI) Ministères

	du champ d'application de certaines administrations		
9	Critères d'identification des entités importantes + Modalités d'exclusion du champ d'application de certaines administrations	Décret en Conseil d'Etat Arrêté	Agence nationale de sécurité des systèmes d'informations (ANSSI) Ministères
10	Mécanismes et modalités de désignation unitaire d'entités importantes ou essentielles	Décret en Conseil d'Etat Arrêté	Agence nationale de sécurité des systèmes d'informations (ANSSI) Ministères
11	Territorialité de l'application de la présente loi aux entités	Néant	Sans objet
12	Remontée d'informations des entités importantes et essentielles en vue de constituer la liste que la France devra communiquer à la Commission européenne	Décret en Conseil d'Etat	Secrétariat général de la défense et de la sécurité nationale (SGDSN) / Agence nationale de sécurité des systèmes d'informations (ANSSI)
13	Dispositions particulières concernant les actes juridiques sectoriels européen qui pourraient s'appliquer en lieu et place de la transposition de NIS2	Néant	Sans objet
14	Application des mesures de sécurité aux entités importantes et essentielles et également les administrations « régalienne », les juridictions administratives et judiciaires	Décret en Conseil d'Etat	Secrétariat général de la défense et de la sécurité nationale (SGDSN) / Agence nationale de sécurité des systèmes d'informations (ANSSI)
15	Mécanismes permettant à une entité importante ou essentielle de se prévaloir de la conformité à un référentiel établi par l'autorité nationale pour démontrer sa conformité aux exigences prévues	Néant	Secrétariat général de la défense et de la sécurité nationale (SGDSN) / Agence nationale de sécurité des systèmes d'informations (ANSSI)

	à l'article 14		
16	Exigences particulières relatives au volet cyber du dispositif de sécurité des activités d'importance vitale et aux systèmes d'information de l'administration supportant des échanges par voie électronique avec leurs usagers ou d'autres administrations	Décret en Conseil d'Etat Arrêté	Secrétariat général de la défense et de la sécurité nationale (SGDSN) / Agence nationale de sécurité des systèmes d'informations (ANSSI)
17	Notifications d'incidents et vulnérabilités importants	Décret en Conseil d'Etat	Secrétariat général de la défense et de la sécurité nationale (SGDSN) / Agence nationale de sécurité des systèmes d'informations (ANSSI)
18	Champs d'application organique de la section relative à l'enregistrement des noms de domaine	Néant	Sans objet
19	Collecte des données nécessaires à l'enregistrement des noms de domaine	Décret en Conseil d'Etat	Secrétariat général de la défense et de la sécurité nationale (SGDSN) / Agence nationale de sécurité des systèmes d'informations (ANSSI) Direction générale des entreprises (DGE)
20	Conservation des données liées à l'enregistrement des noms de domaine	Néant	Sans objet
21	Publication des données liée à l'enregistrement des noms de domaine	Néant	Sans objet
22	Règles d'accès par les agents habilités par l'autorité judiciaire ou par l'autorité nationale de sécurité des systèmes d'information des données liées à	Décret en Conseil d'Etat	Secrétariat général de la défense et de la sécurité nationale (SGDSN) / Agence nationale de sécurité des systèmes d'informations

	l'enregistrement des noms de domaine		(ANSSI)
23	Partage d'informations nécessaires à l'accomplissement de leurs missions respectives entre l'autorité nationale de sécurité des systèmes d'information d'une part et certains organismes d'autre part (par exemple, la CNIL ou autorité compétente au regard d'un acte juridique sectoriel)	Décret en Conseil d'Etat	Secrétariat général de la défense et de la sécurité nationale (SGDSN) / Agence nationale de sécurité des systèmes d'informations (ANSSI)
24	Agrément pour les relais de prévention et de gestion des incidents	Décret en Conseil d'Etat	Secrétariat général de la défense et de la sécurité nationale (SGDSN) / Agence nationale de sécurité des systèmes d'informations (ANSSI)
25	Supervision	Décret en Conseil d'Etat	Secrétariat général de la défense et de la sécurité nationale (SGDSN) / Agence nationale de sécurité des systèmes d'informations (ANSSI)
26	Habilitation des agents amenés à rechercher et constater des manquements, notamment aux dispositions de la présente loi	Décret en Conseil d'Etat	Secrétariat général de la défense et de la sécurité nationale (SGDSN) / Agence nationale de sécurité des systèmes d'informations (ANSSI)
27	Nature des activités de contrôle	Néant	Sans objet
28	Coopération de la personne contrôlée et amende en cas d'obstacle à un contrôle	Néant	Sans objet
29	Nature des activités de contrôle	Néant	Sans objet
30	Modalités d'application de la sous-section 2 de la section 1 du chapitre III (art. 27 à 29)	Décret en Conseil d'Etat	Secrétariat général de la défense et de la sécurité nationale (SGDSN) / Agence

			nationale de sécurité des systèmes d'informations (ANSSI)
31	Ouverture de la procédure	Néant	Sans objet
32	Mesure d'exécution	Néant	Sans objet
33	Notification des griefs et saisine de la commission des sanctions	Néant	Sans objet
34	Modalités d'application de la section 2 du chapitre III (art. 31 à 33)	Décret en Conseil d'Etat	Secrétariat général de la défense et de la sécurité nationale (SGDSN) / Agence nationale de sécurité des systèmes d'informations (ANSSI)
35	Commission des sanctions	Néant	Sans objet
36	Composition de la commission des sanctions	Néant	Sans objet
37	Nature de sanction	Néant	Sans objet
38	Alléger le contrôle des biens de cryptologie	Décret en Conseil d'Etat Décret simple Arrêté	Secrétariat général de la défense et de la sécurité nationale (SGDSN) / Agence nationale de sécurité des systèmes d'informations (ANSSI)
39	Modification de l'ordonnance n° 2005-1516 du 8 décembre 2005, de la loi n° 2018-133 du 3 février 2018, de certaines dispositions du code de la défense et de certaines dispositions du code des postes et des communications électroniques	Décret en Conseil d'Etat	Secrétariat général de la défense et de la sécurité nationale (SGDSN) / Agence nationale de sécurité des systèmes d'informations (ANSSI)
40	Mesures applicables à l'outre-mer pour les territoires sous spécialité législative	Néant	Sans objet
41	Renforcement des sanctions pénales pour améliorer la lutte	Néant	Sans objet

	contre les brouillages		
42	Renforcement des conditions d'accès à une assignation de fréquences déposées par la France auprès de l'Union Internationale des Télécommunications	Décret en Conseil d'Etat	Ministère de l'Economie, des Finances et de la Souveraineté industrielle et numérique / Direction générale des entreprises
43	Modification de la définition des prestataires de services techniques	Néant	Sans objet
44	Maintien de la résilience opérationnelle des gestionnaires de plateformes de négociation	Néant	Sans objet
45	Gestion du risque lié aux technologies de l'information et de la communication par les entreprises de marché	Néant	Sans objet
46	Référence 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	Néant	Sans objet
47	Référence aux réseaux et systèmes d'information au sein des exigences de contrôle interne des établissements de crédit et des sociétés de financement	Néant	Sans objet
48	Obligations des prestataires de services de paiement en matière de gestion du risque lié aux technologies de l'information et des communications (TIC)	Néant	Sans objet
49	Modification de la liste des prestataires de services de paiement soumis à une obligation de notification des incidents opérationnels ou de sécurité majeur	Néant	Sans objet
50	Référence aux réseaux et systèmes d'information au sein des exigences de contrôle et de sauvegarde des prestataires de	Néant	Sans objet

	service d’investissement		
51	Systèmes de technologies de l’information et de la communication (TIC) et dispositifs de contrôle des prestataires de services d’investissement	Néant	Sans objet
52	Systèmes de contrôle des risques mis en œuvre par les prestataires de services d'investissement autres que les sociétés de gestion de portefeuille qui ont recours à la négociation algorithmique	Néant	Sans objet
53	Référence aux prestataires informatiques critiques au sein des tiers auxquels l’Autorité de contrôle prudentiel et de résolution peut demander toute information	Néant	Sans objet
54	Référence à la résilience opérationnelle numérique au sein des plans préventifs de résolution des établissements de crédit et des sociétés de financement	Néant	Sans objet
55	Extension de la liste des autorités habilitées à s’échanger des informations	Néant	Sans objet
56	Modification du code monétaire et financier	Néant	Sans objet
57	Nouvelles obligations pour les entreprises d’assurance et de réassurance en matière de gouvernance des risques liés à l’utilisation des systèmes d’information	Néant	Sans objet
58	Extension aux groupes d’assurance des nouvelles obligations de gouvernance des risques liés à l’utilisation des systèmes d’information	Néant	Sans objet
59	Nouvelles obligations pour les unions et mutuelles du code de la	Néant	Sans objet

	mutualité en matière de gouvernance des risques liés à l'utilisation des systèmes d'information		
60	Suppression de dispositions redondantes dans le code de la mutualité	Néant	Sans objet
61	Nouvelles obligations pour les institutions de prévoyance et unions du code de la sécurité sociale en matière de gouvernance des risques liés à l'utilisation des systèmes d'information	Néant	Sans objet
62	Dates d'application des dispositions du titre III sur la résilience opérationnelle numérique du secteur financier	Néant	Sans objet

TABLEAU D'INDICATEURS

Indicateur	Objectif et modalités de l'indicateur	Objectif visé (en valeur et/ou en tendance)	Horizon temporel de l'évaluation (période ou année)	Identification et objectif des dispositions concernées
Nombre d'opérateurs d'importance vitale désignés par les autorités administratives	L'indicateur vise à mesurer l'augmentation ou la diminution du nombre d'opérateurs d'importance vitale	Légère augmentation du nombre global d'opérateurs d'importance vitale	6 ans	Article 1er Création de l'article L. 1332-2 du code de la défense
Réalisation des plans de résilience opérateurs (PRO)	L'indicateur vise à mesurer de taux de réalisation des PRO	Augmentation du nombre de PRO réalisés par les opérateurs et approuvés par l'administration	6 ans	Article 1er Création de l'article L. 1332-3 du code de la défense
Réalisation des plans particuliers de résilience (PPR)	L'indicateur vise à mesurer de taux de réalisation des PPR	Augmentation du nombre de PPR réalisés par les opérateurs et approuvés par l'administration	6 ans	Article 1er Création de l'article L. 1332-5 du code de la défense
Nombre d'entités importantes et d'entités essentielles enregistrées auprès de	L'indicateur vise à mesurer : Pour la phase de déclaration initiale (0 à 4 mois) suivi du nombre d'entités enregistrées auprès de	En phase de déclaration initiale : Augmentation du nombre d'entité enregistrées	Annuel	Article 8 et 9

l'Agence Nationale de Sécurité des systèmes d'information (ANSSI)	l'ANSSI Puis annuellement suivi des variations du nombre d'assujetti	auprès de l'Agence Nationale de la Sécurité des Systèmes Information Puis : Stabilité de l'indicateur		
Evolution du nombre de notification d'incident par rapport à l'évolution de la menace cyber observée par l'Agence Nationale de Sécurité des Systèmes d'information (ANSSI)	L'indicateur vise à mesurer : Pour la phase de déploiement (0 à 3 ans) : l'augmentation du nombre d'incidents notifiés par les assujettis Pour la phase post déploiement (après 3 ans) : la corrélation entre le nombre d'incidents notifiés et l'évaluation du niveau de menace cyber	Phase de déploiement : Augmentation du nombre d'incidents notifiés Phase post - déploiement : Corrélation entre le nombre d'incident et l'évolution de la menace cybercriminelle	Annuel	Article 17
Nombre de vulnérabilités communiqué publiquement par l'Agence à la place des éditeurs de logiciel par rapport au nombre de vulnérabilités totales rendues publiques	L'indicateur vise à évaluer le taux de signalement de vulnérabilité par les éditeurs de logiciels et ainsi de mesurer le suivi de l'obligation par les éditeurs	Diminution forte du taux de déclaration effectuée par l'ANSSI à la place des éditeurs	Annuel	Article 17
Nombre de mises en	L'indicateur vise évaluer le taux de mise en conformité	Augmentation du taux de mise	3 ans	Articles 27 à 37

demeure et sanctions émises par rapport au nombre de contrôles réalisés par l'Agence Nationale de Sécurité des Systèmes d'information (ANSSI)	des entités	en conformité des entités		

TITRE I^ER – RESILIENCE DES ACTIVITES D'IMPORTANCE VITALE

CHAPITRE I^ER – MODIFICATIONS DU CODE DE LA DEFENSE

Article 1^er – Modifications des articles (articles L. 1332-1 à L. 1332-22 du code de la défense)

Le premier article du projet de loi a pour objectif de modifier l'actuel chapitre II du titre III du Livre III de la partie 1 du code de la défense portant sur la protection des installations d'importance vitale (L. 1332-1 à L. 1332-7). Ce chapitre devant s'intituler « Résilience des activités d'importance vitale » sera composé de trois sections et comportera 22 articles.

Article 1^er (A) – Article L. 1332-1 du code de la défense – Définitions

1. ETAT DES LIEUX

1.1. CADRE GENERAL

En France, le dispositif national de sécurité des activités d'importance vitale (SAIV) a été créé en 2006 sur les bases 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. Cette première réforme visait notamment une simplification et une rationalisation du processus, en passant de trois niveaux de sensibilité des sites à un régime unique, et en concentrant l'effort sur un nombre resserré d'établissements (passage d'environ 4000 à 1500 points d'importance vitale).

Cette politique publique a été conçue dans un contexte de menace terroriste croissante, à la suite, notamment, des attentats de Madrid (2004) et de Londres (2005).

L'actuel dispositif de sécurité des activités d'importance vitale vise à assurer la protection physique et cyber d'opérateurs (publics ou privés) identifiés comme indispensables pour la

continuité d'activité de la Nation, ou, de manière plus marginale, pouvant présenter un danger grave pour la population.

Ce dispositif est inscrit dans le code de la défense (articles L. 1332-1 à L. 1332-7) et compte aujourd'hui plus de 300 opérateurs, désignés d'importance vitale par l'Etat, dans 12 secteurs d'activité. Chaque secteur est supervisé par un ministère coordonnateur.

Actuellement, les articles L. 1332-1 et L. 1332-2 du code de la défense définissent une activité d'importance vitale, bien que la notion n'apparaisse pas en tant que telle :

Article L. 1332-1 : « Les opérateurs publics ou privés exploitant des établissements ou utilisant des installations et ouvrages, dont l'indisponibilité risquerait de diminuer d'une façon importante le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la nation, sont tenues 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. Ces établissements, installations ou ouvrages sont désignés par l'autorité administrative. »

Article L. 1332-2 : « Les obligations prescrites par le présent chapitre 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. Ces établissements sont désignés par l'autorité administrative. »

L'article R. 1332-4, par renvoi au R. 1332-1, définit les points d'importance vitale comme les « établissements ou ouvrages, une ou des installations dont le dommage ou l'indisponibilité ou la destruction par suite d'un acte de malveillance, de sabotage ou de terrorisme risquerait, directement ou indirectement,

a) D'obérer gravement le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la Nation ;

b) Ou de mettre gravement en cause la santé ou la vie de la population. ».

1.2. CADRE CONSTITUTIONNEL

Aux termes de l'article 88-1 de la Constitution : « La République participe aux Communautés européennes et à l'Union européenne, constituées d'Etats qui ont choisi librement, en vertu des traités qui les ont instituées, d'exercer en commun certaines de leurs compétences ». Le Conseil constitutionnel déduit de cette disposition que : « la transposition en droit interne

d'une directive communautaire résulte d'une exigence constitutionnelle »[2]. Il en va de même pour une loi ayant pour objet d'adapter le droit interne à un règlement de l'Union européenne[3].

Le dispositif de la SAIV institué en France à partir de 2006 était spécifique à la France et s'inscrivait dans le cadre constitutionnel ordinaire.

Par ailleurs, les définitions participent de l'intelligibilité et de l'accessibilité de la lois, objectifs à valeur constitutionnels qui découlent des articles 4, 5, 6 et 16 de la Déclaration des droits de l'Homme et du Citoyen de 1789[4].

1.3. CADRE CONVENTIONNEL

Au niveau européen, avant l'adoption de la directive (UE) 2022/2557 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience des entités critiques (REC), le seul cadre conventionnel applicable était la directive 2008/114/CE du Conseil du 8 décembre 2008 concernant le recensement et la désignation des infrastructures critiques européennes ainsi que l'évaluation de la nécessité d'améliorer leur protection, limitée aux secteurs des transports et de l'énergie.

La directive REC du 14 décembre 2022 doit être transposée dans notre droit national d'ici le 17 octobre 2024. Elle vise à améliorer la fourniture, dans le marché intérieur, de services essentiels au maintien de fonctions sociétales ou d'activités économiques vitales en renforçant la résilience des opérateurs (appelés entités) critiques qui fournissent de tels services.

La directive REC remplace et refond en profondeur la directive de 2008 :

- elle prévoit le passage d'une logique de protection physique d'infrastructures à une logique de résilience et de continuité d'activité ;
- elle vise les « entités critiques » nationales (c'est-à-dire les opérateurs), et non plus seulement les infrastructures critiques européennes (c'est-à-dire celles dont l'arrêt ou la destruction aurait un impact sur au moins deux États membres) ;
- elle s'inscrit dans une politique de résilience globale et cohérente puisque les entités critiques seront également soumises aux obligations de cyber-résilience prévues par la directive NIS 2 ;

[2] Voir notamment la décision n° 2004-496 DC du 10 juin 2004, « Loi pour la confiance dans l'économie numérique ».

[3] Voir par exemple la décision n° 2018-765, « Loi relative à la protection des données personnelles », considérant 3.

[4] Décision 2013-685 DC du 29 décembre 2013.

– elle élargit le nombre de secteurs concernés. Le champ d'application couvre désormais 11 secteurs, qui correspondent presque parfaitement aux secteurs actuels de la SAIV : énergie, transports, infrastructures bancaires, infrastructures de marché financier, santé, eau potable, assainissement, infrastructures digitales, administration publique (niveau central), espace, alimentation.

La directive permet d'offrir un socle minimal commun de résilience à tous les opérateurs de l'UE. Ces derniers ne sont aujourd'hui pas tous couverts par un dispositif comparable à celui mis en œuvre en France, ce qui rétablira une forme de concurrence loyale à l'échelle européenne.

L'article 2 de la directive REC établit les définitions suivantes :

> « 1) « entité critique », une entité publique ou privée qui a été désignée par un État membre conformément à l'article 6 comme appartenant à l'une des catégories qui figurent dans la troisième colonne du tableau de l'annexe;
>
> 2) « résilience », la capacité d'une entité critique à prévenir tout incident, à s'en protéger, à y réagir, à y résister, à l'atténuer, à l'absorber, à s'y adapter et à s'en rétablir;
>
> 3) « incident », un événement qui perturbe ou est susceptible de perturber de manière importante la fourniture d'un service essentiel, y compris lorsqu'il affecte les systèmes nationaux qui préservent l'état de droit ;
>
> 4) « infrastructure critique », un bien, une installation, un équipement, un réseau ou un système, ou une partie d'un bien, d'une installation, d'un équipement, d'un réseau ou d'un système, qui est nécessaire à la fourniture d'un service essentiel ;
>
> 5) « service essentiel », un service qui est crucial pour le maintien de fonctions sociétales ou d'activités économiques vitales, de la santé publique et de la sûreté publique, ou de l'environnement ;
>
> 6) « risque », le potentiel de perte ou de perturbation causé par un incident, à exprimer comme la combinaison de l'ampleur de cette perte ou de cette perturbation et la probabilité que l'incident se produise;
>
> 7) « évaluation des risques », l'ensemble du processus permettant de déterminer la nature et l'étendue d'un risque en déterminant et en analysant les menaces, les vulnérabilités et les dangers potentiels pertinents qui pourraient conduire à un incident et en évaluant la perte ou la perturbation potentielle de la fourniture d'un service essentiel causée par cet incident ;
>
> 8) « norme », une norme au sens de l'article 2, point 1), du règlement (UE) n° 1025/2012 du Parlement européen et du Conseil (30) ;

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

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

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

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

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

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

1.4. ELEMENTS DE DROIT COMPARE

1.4.1. Le cas européen

Les autres Etats membres de l'Union européenne feront évoluer leur législation et adopteront des définitions similaires ou conformes à celles de la directive REC. A titre d'exemple, le Luxembourg a reproduit à l'identique les définitions mentionnées dans la directive REC[5].

1.4.2. Le cas américain

Les Etats-Unis ont été précurseurs dans l'élaboration des notions d'activité d'importance vitale et d'infrastructure critique. Ce mouvement de conceptualisation fait notamment suite aux attentats du 11 septembre 2001 au *World Trade Center* à New-York.

Le droit américain, notamment dans le *Patriot Act*, définit les infrastructures critiques comme « les systèmes et les biens, physiques ou virtuels, qui sont si vitaux pour les États-Unis que l'incapacité ou la destruction de tels systèmes ou biens aurait un effet incapacitant sur la

[5] 289176.pdf (chd.lu).

sécurité économique nationale, la santé publique nationale ou la sûreté, ou toute combinaison de ces questions ».

1.4.3. Le cas canadien

Les autorités canadiennes mettent l'accent sur l'impact potentiel sur la population nationale de la dégradation ou de l'absence de certaines activités essentielles. Les « infrastructures essentielles » sont définies comme étant « les installations matérielles et informatiques, les réseaux, les services et les biens matériels dont la perturbation ou la destruction aurait de sérieuses conséquences pour la santé, la sécurité ou le bien-être économique des Canadiens et des Canadiennes, ou pour le fonctionnement efficace des gouvernements au Canada ».

2. NECESSITE DE LEGIFERER ET OBJECTIFS POURSUIVIS

2.1. NECESSITE DE LEGIFERER

Afin de mettre en conformité le droit national et le droit européen, tel qu'il résulte de la directive (UE) 2022/2557 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience des entités critiques, il est nécessaire de modifier les définitions actuellement applicables. Les dispositions envisagées visent à articuler les définitions nationales de la SAIV (activité d'importance vitale, infrastructure critique, point d'importance vitale (PIV) et système d'information d'importance vitale (SIIV)) avec la définition de l'infrastructure critique fixée dans la directive REC. En effet, l'actuelle définition de la SAIV n'était pas assez complète (centrée sur la défense et la sécurité nationale, alors que la notion européenne de service essentiel est centrée sur la continuité économique (du marché intérieur)) et devait être simplifiée.

La nécessité d'inscrire dans la loi ces définitions résulte de l'application de l'article 34 de la Constitution, dès lors qu'elle peut être regardée comme déterminant un principe fondamental d'organisation de la défense nationale et que ces mentions concernent le champ d'application des obligations prévues par la directive dont la méconnaissance pourrait donner lieu à des sanctions administratives.

C'est également une exigence de clarté et d'accessibilité qui commande cette inscription.

2.2. OBJECTIFS POURSUIVIS

Il s'agit à la fois de simplifier les définitions actuelles et de les mettre en cohérence avec le nouveau lexique prévu par la directive, en précisant la définition des activités d'importance vitale ainsi qu'en insérant dans le droit national les notions d'infrastructure critique, issue de

la directive, et d'y inclure les points d'importance vitale et les systèmes d'information d'importance vitale.

3. OPTIONS ENVISAGEES ET DISPOSITIF RETENU

3.1. OPTIONS ENVISAGEES

Le Gouvernement a envisagé de reprendre directement les notions issues de la directive et de les substituer aux définitions actuelles. Toutefois, lors des travaux d'élaboration du projet de loi, cette option a été écartée pour pouvoir continuer à distinguer, parmi les infrastructures critiques, les points véritablement les plus sensibles.

Il a donc été privilégier de s'adosser sur le dispositif existant qui fonctionne et qui est connu des opérateurs.

3.2. DISPOSITIF RETENU

Les nouvelles dispositions envisagées conservent le vocabulaire national, de même que la logique d'identification de l'ensemble des sites les plus sensibles (points d'importance vitale) ainsi que la planification associée. En effet, la directive ne prévoit des plans qu'à l'échelle de l'opérateur lui-même (plan de résilience), lorsque le dispositif national existant repose également sur des plans détaillés relatifs à chaque point d'importance vitale. Cette logique de double niveau est conservée pour ne pas diminuer le niveau d'exigence appliqué à nos opérateurs les plus sensibles.

L'objectif est de simplifier et d'élargir la définition des activités d'importance vitale par rapport à la rédaction actuelle, en veillant à la cohérence d'ensemble avec la définition fixée dans la directive REC.

Concernant la définition d'infrastructure critique, la définition proposée au présent article entend l'infrastructure critique comme une catégorie générique englobant les points d'importance vitale (PIV) et les systèmes d'information d'importance vitale (SIIV).

D'un point de vue opérationnel, la volonté de conservation du vocable national a pour objectif de simplifier la transposition de la directive européenne pour l'ensemble des parties prenantes au dispositif.

4. ANALYSE DES IMPACTS DES DISPOSITIONS ENVISAGEES

4.1. IMPACTS JURIDIQUES

4.1.1. Impact sur l'ordre juridique interne

La présente mesure crée un nouvel article L. 1332-1 du code de la défense au sein au sein d'un Chapitre II renommé « Résilience des activités d'importance vitale » (et non plus « Protection des installations d'importance vitale »), avec une section 1 rebaptisée « Dispositions générales relatives aux activités d'importance vitale » (et non plus « Dispositions générales »).

Prise seule, cette disposition ne fixe aucune obligation mais permet de rendre intelligibles et accessibles des notions connues au regard des nouvelles exigences et formulations imposées par la directive.

L'intelligibilité et l'accessibilité de la loi sont bien des objectifs à valeur constitutionnels poursuivis par le législateur en conformité avec ces objectifs qui découlent des articles 4, 5, 6 et 16 de la Déclaration des droits de l'Homme et du Citoyen de 1789[6].

4.1.2. Articulation avec le droit international et le droit de l'Union européenne

Le présent article entend mettre les définitions nationales relatives aux activités d'importance vitale en conformité avec les dispositions retenues dans la directive européenne REC.

4.2. IMPACTS ECONOMIQUES ET FINANCIERS

4.2.1. Impacts macroéconomiques

Les mesures de résilience prévues pourront engendrer des coûts supplémentaires pour un opérateur. Si la logique de protection physique était déjà prise en compte, la systématisation de la prise en compte de la continuité d'activité ne sera en effet pas neutre. Ces coûts sont extrêmement difficiles à évaluer tant les opérateurs de la SAIV opèrent dans des secteurs diversifiés et à différentes échelles.

Néanmoins, le principe de résilience – au cœur de cette transposition – permettra *in fine* à l'opérateur et – au regard de certaines dépendances – à l'ensemble du tissu économique, de pouvoir maintenir son activité dans un contexte dégradé et vise à amortir les coûts imputables à la disruption de son activité. En effet, l'ensemble des activités d'importance vitale sont nécessaires à l'activité économique de la nation (transports, énergie, télécommunications…) voire à la société elle-même (alimentation, activités civiles et militaires de l'Etat…).

4.2.2. Impacts sur les entreprises

[6] Décision 2013-685 DC du 29 décembre 2013.

Sans objet.

4.2.3. Impacts budgétaires

Sans objet.

4.3. IMPACTS SUR LES COLLECTIVITES TERRITORIALES

Les collectivités territoriales désignées opérateurs d'importance vitale devront, comme c'est déjà le cas dans le dispositif actuel, désigner des PIV et des SIIV.

4.4. IMPACTS SUR LES SERVICES ADMINISTRATIFS

Les services administratifs de l'Etat (préfectures, ministères coordonnateurs, SGDSN) sont chargés d'identifier et de désigner les opérateurs d'importance vitale.

Bien que la terminologie évolue, les nouvelles définitions européennes transposées en droit français reprennent l'essence des dispositions actuellement en vigueur. L'impact sur les services administratifs reste ainsi nominal.

4.5. IMPACTS SOCIAUX

4.5.1. Impacts sur la société

Le renforcement des exigences en matière de résilience des activités d'importance vitale doit permettre de limiter les impacts d'une crise ou de problèmes majeurs d'un opérateur d'importance vitale sur le fonctionnement de la société.

4.5.2. Impact sur les personnes en situation en handicap

Sans objet.

4.5.3. Impacts sur l'égalité entre les femmes et les hommes

Sans objet.

4.5.4. Impacts sur la jeunesse

Sans objet.

4.5.5. Impacts sur les professions réglementées

Sans objet.

4.6. IMPACTS SUR LES PARTICULIERS

Sans objet.

4.7. IMPACTS ENVIRONNEMENTAUX

Le dispositif conserve la catégorie spécifique des opérateurs industriels à haut-risque, notamment à des fins de protection de l'environnement. Certaines installations peuvent avoir des impacts (pollution de l'eau, de l'air, des sols, …et présenter des dangers (incendie, explosion, etc.) pour l'environnement, la santé et la sécurité publique. Certains établissements classés ICPE peuvent donc être désignés OIV (voir schémas au 1.1.2 de ce chapitre).

L'objectif de ce dispositif est également, comme c'est le cas depuis 2013, de protéger les OIV face aux risques naturels (inondations, incendie, etc.)

5. CONSULTATIONS MENEES ET MODALITES D'APPLICATION

5.1. CONSULTATIONS MENEES

Une concertation de l'ensemble des ministères coordonnateurs a été réalisée sur cette mesure.

En application de l'article L. 1212-2 du code général des collectivités territoriales, le présent article a été soumis à l'examen du Conseil national d'évaluation des normes qui a rendu un avis défavorable le 22 mai 2024.

Enfin, le service national des enquêtes administratives de sécurité, le coordinateur général de la sécurité nucléaire, le service juridique du Secrétariat général des affaires européennes et l'Agence nationale de sécurité des systèmes d'informations ont également été consultés.

5.2. MODALITES D'APPLICATION

5.2.1. Application dans le temps

Les présentes dispositions entrent en vigueur le lendemain de la publication de la présente loi au *Journal officiel* de la République française.

5.2.2. Application dans l'espace

Le présent titre du présent projet de loi vise à créer 22 articles au sein du code de la défense, qui est applicable de plein droit sur l'ensemble du territoire de la République conformément à son article L. 1.

Aussi, les dispositions du code de la défense créées par le présent projet de loi seront applicables de plein droit à la fois dans les collectivités régies par le principe de l'identité législative (la Guadeloupe, la Guyane, la Martinique, La Réunion, Mayotte, Saint-Barthélemy, Saint-Martin et Saint-Pierre-et-Miquelon) et par le principe de la spécialité législative (les îles Wallis et Futuna, la Polynésie française, la Nouvelle-Calédonie et les Terres australes et antarctiques françaises).

Les nouveaux articles L. 1332-2 et L. 1332-3 du code de la défense renvoient à des dispositions du code de l'environnement qui ne sont pas applicables à Saint-Barthélemy, dans les îles Wallis et Futuna, en Polynésie française, en Nouvelle-Calédonie et dans les Terres australes et antarctiques françaises, les collectivités étant compétentes dans cette matière. Si l'article L. 6311-1 du code de la défense prévoit déjà une grille de lecture générale qui couvre toute la partie législative pour son application dans les îles Wallis et Futuna, en Polynésie française, en Nouvelle-Calédonie et dans les Terres australes et antarctiques françaises, il n'existe de grille similaire pour Saint-Barthélemy. Il est proposé de créer une grille sur le même modèle au sein d'un nouvel article L. 6221-2 du code de la défense, par l'article 3 du présent projet de loi.

Par ailleurs, en tant que PTOM, le droit de l'union européenne ne s'applique pas à Saint-Barthélemy, Saint-Pierre-et-Miquelon, dans les îles Wallis et Futuna, en Polynésie française, Nouvelle-Calédonie et dans les Terres australes et antarctiques françaises. Les dispositions applicables aux seuls OIV exerçant des services essentiels au fonctionnement du marché intérieur de l'Union européenne ne seront donc pas applicables en l'absence d'adaptation.

5.2.3. Textes d'application

Le présent article ne requiert aucun texte d'application.

Article 1er (B) – Article L. 1332-2 du code de la défense – Désignation des OIV

1. ETAT DES LIEUX

1.1. CADRE GENERAL

Dans le cadre du dispositif actuel de sécurité des activités d'importance vitale (SAIV), les articles L. 1332-1 et L. 1332-2 ainsi que l'article R. 1332-3 du code de la défense précisent les dispositions relatives à la désignation des opérateurs d'importance vitale (OIV).

1.1.1. Critères de désignation d'un OIV

Aujourd'hui, le statut d'OIV repose sur deux conditions :

- l'activité de l'opérateur doit s'exercer pour tout ou partie dans un secteur d'activités d'importance vitale ;
- l'opérateur doit gérer ou utiliser au moins un établissement, un ouvrage ou une installation dont le dommage, l'indisponibilité ou la destruction par suite d'un acte de malveillance, de sabotage ou de terrorisme risquerait de quelque manière que ce soit d'avoir des conséquences majeures sur le potentiel de guerre ou économique, la sécurité ou les capacités de survie de la Nation, ou sur la santé ou la vie de la population (article R. 1332-1 du code de la défense). Il s'agit ici des installations industrielles à haut risque.

L'appréciation du caractère d'importance vitale, lié aux conséquences graves d'une menace plausible pour un opérateur, se fonde sur les critères définis par les différentes directives nationales de sécurité (DNS) élaborées par les ministères coordonnateurs pour chaque secteur et sous-secteur d'activité concerné.

Périmètre des entités susceptibles d'être désignées OIV

De manière générale, et sans préjudice des précisions sectorielles apportées par les directives nationales de sécurité (DNS), un OIV peut être :

- une société (société-mère ou filiale) ;
- une association, une fondation ou une organisation internationale ;
- un service de l'Etat, une collectivité territoriale, un groupement de collectivités, un établissement public, une autorité administrative indépendante.

Le choix de l'entité *ad hoc* se fait après concertation avec l'opérateur concerné, en prenant en compte :

- son organisation de la sûreté-sécurité pour répondre au mieux aux objectifs du dispositif SAIV ;
- le lien entre l'entité retenue et les installations, établissements ou ouvrages susceptibles d'être désignés PIV. Ainsi, plusieurs filiales d'un même groupe peuvent, le cas échéant, être désignées.

Notification de la désignation à l'OIV

L'autorité administrative désigne l'OIV par un arrêté, qui doit préciser le ou les secteurs de rattachement (article R. 1332-3 du code de la défense) ainsi que la ou les DNS applicables (article R. 1332-17 du code de la défense).

Les opérateurs coopèrent ensuite, à leurs frais, au dispositif SAIV (article L. 1332-1 du code de la défense).

1.1.2. Processus de désignation d'un opérateur d'importance vitale (OIV)

L'article R. 1332-3 du code de la défense prévoit qu'un opérateur d'importance vitale (OIV) est désigné comme tel par le ministre coordonnateur de son secteur d'activités d'importance vitale, en concertation avec le ou les ministres intéressés et après avis de la commission interministérielle de défense et de sécurité (CIDS) ou de la commission zonale de défense et de sécurité (CZDS).

La notification à l'opérateur de l'intention de le désigner OIV est l'occasion d'une concertation entre l'autorité administrative (ministre coordonnateur ou préfet de département selon le cas) et l'opérateur. Dans les deux mois dont il dispose pour faire ses remarques, l'opérateur peut faire connaître à l'autorité administrative ayant émis la notification, la liste et la nature des infrastructures qu'il pourrait par la suite proposer en annexe de son plan de sécurité d'opérateur (PSO). Il convient de souligner que les OIV relevant du ministère chargé de la défense ne peuvent être désignés que par le ministre chargé de la défense.

Ce principe de désignation comporte une exception mentionnée au deuxième alinéa de l'article R. 1332-3 du code de la défense, s'agissant des OIV qui gèrent exclusivement un établissement mentionné à l'article L. 511-1 du code de l'environnement (installations classées pour la protection de l'environnement) ou comprenant une installation nucléaire de base visée à l'article L. 593-2 du code de l'environnement.

Le préfet de département peut ainsi s'appuyer sur les DNS pour identifier les opérateurs qui pourraient répondre aux critères permettant de les nommer. Dans ce cas, l'OIV est désigné par le préfet du département dans le ressort duquel se trouve cet établissement, après avis de la

CZDS des secteurs d'activités d'importance vitale, et information du ou des ministres coordonnateurs concernés.

Schéma 1 : Désignation d'un OIV – Processus initié par un ministre coordonnateur

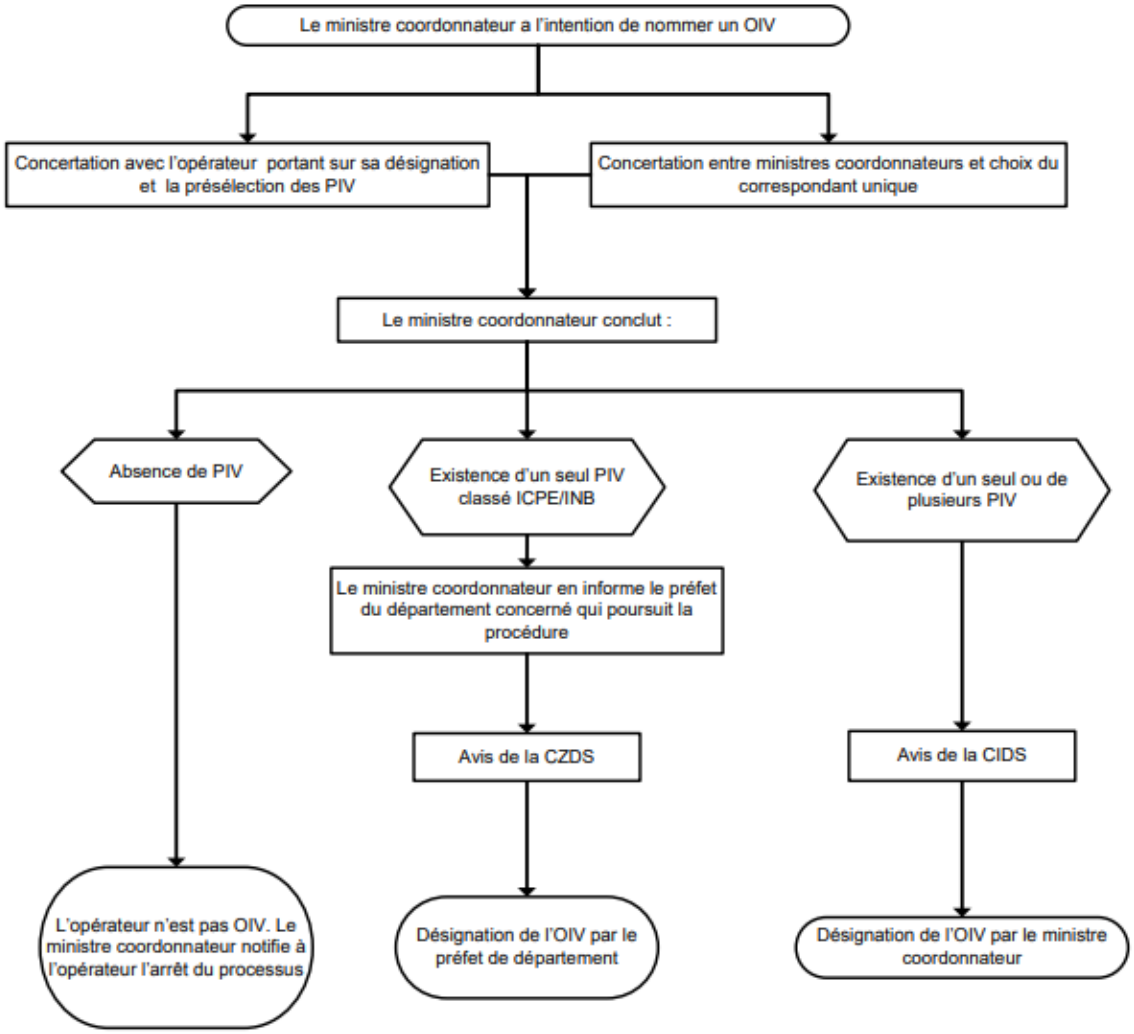
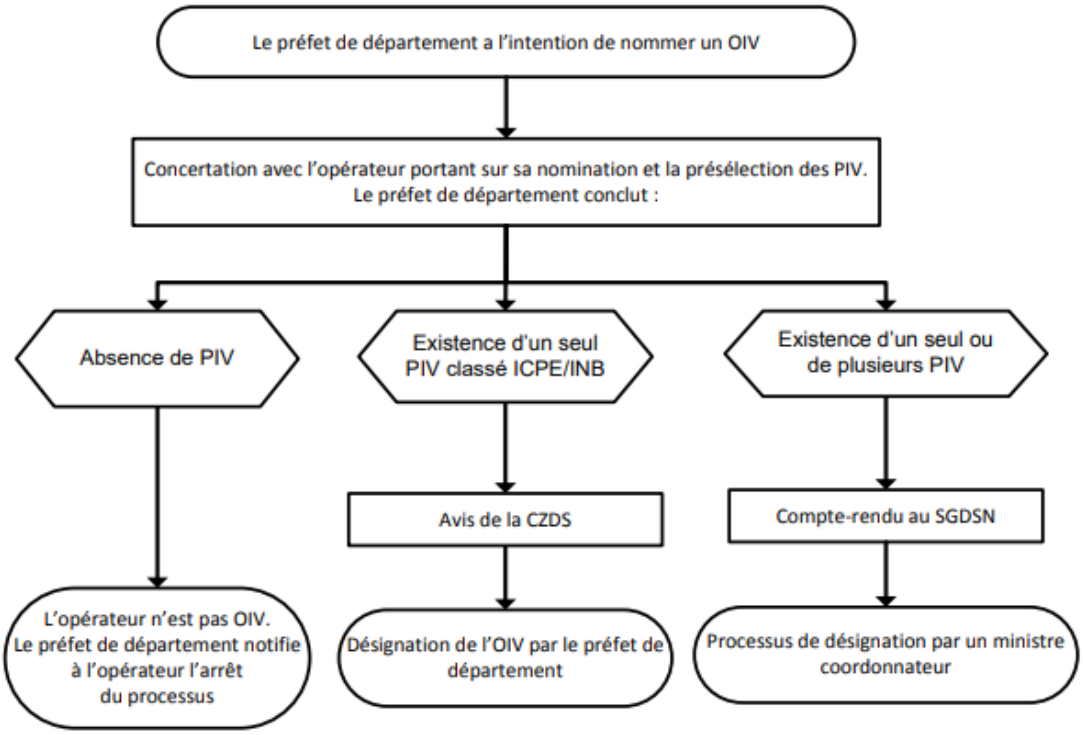


Schéma 2 : Désignation d'un OIV – Processus initié par un préfet de département



1.2. CADRE CONSTITUTIONNEL

Aux termes de l'article 88-1 de la Constitution : « La République participe aux Communautés européennes et à l'Union européenne, constituées d'Etats qui ont choisi librement, en vertu des traités qui les ont instituées, d'exercer en commun certaines de leurs compétences ». Le Conseil constitutionnel déduit de cette disposition que : « la transposition en droit interne d'une directive communautaire résulte d'une exigence constitutionnelle »[7]. Il en va de même pour une loi ayant pour objet d'adapter le droit interne à un règlement de l'Union européenne[8].

La désignation en tant qu'OIV impliquant des obligations à la charge des opérateurs dont le manquement peut être sanctionné au niveau administratif, cette désignation porte nécessairement une atteinte à la liberté d'entreprendre, laquelle découle de l'article 4 de la

[7] Voir notamment la décision n° 2004-496 DC du 10 juin 2004, « Loi pour la confiance dans l'économie numérique ».

[8] Voir par exemple la décision n° 2018-765, « Loi relative à la protection des données personnelles », considérant 3.

Déclaration des droits de l'Homme et du Citoyen de 1789[9]. Cette atteinte ne peut être ni générale ni absolue[10].

En effet, le législateur peut limiter l'exercice de cette liberté à la condition qu'il n'en résulte pas d'atteintes disproportionnées au regard de l'objectif poursuivi[11], alors même que cette atteinte résulterait de l'exigence constitutionnelle de transposition adéquate des directives européennes[12], dans un objectif de sécurité et de défense de la Nation[13], en l'absence de disposition spécifique contraire de la Constitution[14] ou de mise en cause d'une règle ou d'un principe inhérent à notre identité constitutionnelle[15].

Enfin, en l'absence de remise en cause de ses garanties fondamentales, la liberté du commerce et de l'industrie ne s'oppose pas à l'intervention du législateur dans ce domaine[16].

1.3. CADRE CONVENTIONNEL

Au niveau européen, la directive (UE) 2022/2557 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience des entités critiques (REC) permet désormais d'offrir un socle minimal commun de résilience à tous les opérateurs de l'UE. Elle doit être transposée dans notre droit national d'ici le 17 octobre 2024.

Dans son considérant 2[17], la directive REC rappelle que : « La directive 2008/114/CE[18] du Conseil établit une procédure de désignation des infrastructures critiques européennes dans les secteurs de l'énergie et des transports ont la perturbation ou la destruction aurait un impact transfrontière significatif sur deux États membres au moins. Cette directive vise exclusivement la protection de ces infrastructures. Toutefois, l'évaluation de la directive 2008/114/CE réalisée en 2019 a montré qu'en raison de la nature de plus en plus interconnectée et transfrontière des activités faisant appel à des infrastructures critiques, les mesures de protection portant sur des biens individuels ne suffisent pas à elles seules pour empêcher toute perturbation. »

---

[9] Conseil constitutionnel, décision 98-401 DC du 10 juin 1998.

[10] Décision 82-141 DC du 27 juillet 1982.

[11] Décision 2023-1055 QPC du 16 juin 2023.

[12] Décision 2006-535 DC du 30 mars 2006.

[13] Décision 2020-882 QPC du 5 février 2021.

[14] Décision 2004-497 DC du 1er juillet 2004.

[15] Décision 2018-765 DC du 12 juin 2018 ; décision 2019-818 QPC du 6 décembre 2019.

[16] Décision 2003-474 DC du 17 juillet 2003.

[17] https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32022L2557.

[18] Directive 2008/114/CE du Conseil du 8 décembre 2008 concernant le recensement et la désignation des infrastructures critiques européennes ainsi que l'évaluation de la nécessité d'améliorer leur protection.

La directive REC vise donc désormais les « entités critiques » nationales (c'est-à-dire les opérateurs), et non plus seulement les infrastructures critiques européennes. Son champ d'application couvre 11 secteurs : énergie, transports, infrastructures bancaires, infrastructures de marché financier, santé, eau potable, assainissement, infrastructures digitales, administration publique (niveau central), espace, alimentation.

Par ailleurs, la directive REC consacre le passage d'une logique de protection d'infrastructures critiques physiques à une logique de résilience des entités critiques (article 1er), qui met davantage l'accent sur la continuité de leur activité, en sus de la protection physique de leurs installations.

Dans son article 6 (paragraphe 2), la directive européenne REC identifie les critères suivants pour le recensement des entités critiques :

> « a) l'entité fournit un ou plusieurs services essentiels ;
>
> b) l'entité exerce ses activités sur le territoire dudit État membre et son infrastructure critique est située sur ledit territoire ; et
>
> c) un incident aurait des effets perturbateurs importants, déterminés conformément à l'article 7, paragraphe 1, sur la fourniture par l'entité d'un ou de plusieurs services essentiels ou sur la fourniture d'autres services essentiels dans les secteurs figurant à l'annexe qui dépendent dudit ou desdits services essentiels. »

1.4. ELEMENTS DE DROIT COMPARE

Sans objet.

2. NECESSITE DE LEGIFERER ET OBJECTIFS POURSUIVIS

2.1. NECESSITE DE LEGIFERER

La nécessité de légiférer procède de la prise en compte de la notion de « résilience » qui figure expressément dans la directive REC mais n'existe pas dans la règlementation nationale en vigueur.

En application de l'article premier de la directive REC :

« La présente directive :

a) impose aux États membres l'obligation d'adopter des mesures spécifiques visant à garantir que les services qui sont essentiels au maintien de fonctions sociétales ou

d'activités économiques vitales, dans le champ d'application de l'article 114 du traité sur le fonctionnement de l'Union européenne, soient fournis sans entrave dans le marché intérieur, en particulier l'obligation de recenser les entités critiques et l'obligation d' aider les entités critiques à s'acquitter des obligations qui leur incombent ;

b) **impose aux entités critiques des obligations visant à renforcer leur résilience** et leur capacité à fournir les services visés au point a) dans le marché intérieur ; […] ».

Par ailleurs, l'article 34 de la Constitution prévoit que « la loi détermine les principes fondamentaux ([...)] de la libre administration des collectivités territoriales, de leurs compétences et de leurs ressources », témoignant de la nécessité de légiférer dans le présent cas lorsqu'une collectivité territoriale est concernée. Par ailleurs, ces dispositions ayant nécessairement un impact sur la liberté d'entreprendre et la liberté du commerce et de l'industrie, elles relèvent du niveau législatif.

2.2. OBJECTIFS POURSUIVIS

Le premier objectif poursuivi par la rédaction de cet article est de conserver les grands principes du dispositif actuel de la SAIV tout en incluant une dimension résilience à la désignation des opérateurs. Cette intégration s'accompagne également d'une clarification sur la compatibilité de la notion d'OIV avec celle d'entité critique au sens de la directive.

En effet, dès lors que l'activité exercée constitue un service essentiel au fonctionnement du marché intérieur de l'Union européenne, alors l'OIV est une entité critique.

Par ailleurs, un second objectif consiste à améliorer la communication – dans le respect du secret de la défense nationale – entre délégant et délégataire en vue de rendre le dispositif SAIV lui-même plus résilient. En effet, au cours de consultations menées avec les ministères dans le cadre des travaux de transposition, il est apparu que, dans le cas des délégations et des contrats d'exploitation au profit de collectivités territoriales, les délégants peuvent se retrouver insuffisamment inclus dans le processus de désignation. Ces derniers n'étant pas toujours informés du statut du délégataire, le contrôle de l'allocation des ressources à l'application des dispositions prévues dans le cadre de la SAIV n'était pas toujours effectué.

3. OPTIONS ENVISAGEES ET DISPOSITIF RETENU

3.1. OPTION ENVISAGE

Il a été envisagé la possibilité de conférer aux collectivités locales délégantes le statut d'OIV dans la mesure où les délégants sont en majorité des collectivités territoriales, notamment

dans les secteurs de l'eau et des transports collectifs. Toutefois, à des fins de simplification du dispositif, le Gouvernement ne souhaite pas ajouter un échelon supplémentaire au sein des OIV en créant un statut d'OIV spécifique applicable aux seules collectivités territoriales concernées (elles n'auraient, en effet, pas été concernées par l'intégralité des obligations pesant sur les autres OIV).

3.2. DISPOSITIF RETENU

Les dispositions envisagées visent à clarifier la désignation des OIV par l'autorité administrative, à conserver la particularité des opérateurs désignés au titre du danger grave pour la population (installation classées pour la protection de l'environnement au titre Ier du livre V du code de l'environnement ; dispositions relatives aux installation nucléaires de base prévues au chapitre III du titre IX du livre V du même code)et à ajouter une obligation d'information au profit des collectivités territoriales.

Au I, les principes actuels de désignation d'un OIV, fondé sur deux types d'opérateurs, ont été conservés :

- la définition prévue au 1° concerne les OIV exerçant une « activité d'importance vitale dont les activités sont indispensables au fonctionnement de l'économie, de la société, à la défense ou à la sécurité de la nation » : la définition a été simplifiée par rapport à la rédaction actuellement en vigueur afin de mieux prendre en compte les enjeux de continuité d'activité, tout en s'alignant sur les critères prévus par la directive. Dès lors qu'ils exercent une activité qui constitue un service essentiel au fonctionnement du marché intérieur de l'Union européenne, alors l'OIV est une entité critique
- la définition prévue au 2° concerne les OIV les opérateurs désignés au titre du danger grave pour la population (installation classées pour la protection de l'environnement au titre Ier du livre V du code de l'environnement ; dispositions relatives aux installation nucléaires de base prévues au chapitre III du titre IX du livre V du même code)qui pourront connaître des aménagement dans les mesures applicables, afin que ces opérateurs privilégient les impératifs de sécurité sur la continuité d'activité.

La deuxième partie de l'article (II) concerne l'obligation d'information au profit des collectivités territoriales.

4. ANALYSE DES IMPACTS DES DISPOSITIONS ENVISAGEES

4.1. IMPACTS JURIDIQUES

4.1.1. Impact sur l'ordre juridique interne

Les présentes dispositions remplacent l'actuel article L. 1332-2 du code de la défense, au sein du Chapitre II « Résilience des activités d'importance vitale ».

Ainsi que mentionné précédemment, ces dispositions, dont le principe existait déjà, portent une atteinte à la liberté d'entreprendre et à la liberté du commerce et de l'industrie qui est proportionnée et en rapport avec l'objectif poursuivi se rattachant à la défense et à la sécurité nationale.

Par ailleurs, le remplacement des dispositions des actuels articles L. 1332-1 et L. 1332-2 du code de la défense implique d'en tirer les conséquences dans les dispositions de droit interne qui font référence, selon les cas, à certains établissements, installations ou ouvrages, relevant de l'article L. 1332-1 (actuel), lesquels correspondront aux infrastructures critiques des opérateurs d'importance vitale.

Cet impact ne se limite pas aux seuls établissements, installations, ouvrages mais peut également concerner les opérateurs eux-mêmes, lesquels seront désormais qualifiés par la loi d'opérateurs d'importance vitale qui seront distincts selon les modalités de désignation, au titre du 1° ou du 2° du I de l'article L. 1332-2.

Enfin, les modifications prévues s'agissant des documents de planification ont entraîné des impacts sur les dispositions internes y faisant référence.

Toutes ces modifications induites ont été regroupées au sein d'un article 2, qui procède aux modifications nécessaires. Ces dispositions n'ont par elles-mêmes aucun autre impact que celui de modifier des références textuelles.

4.1.2. Articulation avec le droit international et le droit de l'Union européenne

La présente disposition décline au niveau national l'obligation d'identification des entités critiques en adaptant les terminologies retenues dans la directive « REC » (notamment à son article 1er) avec celles actuellement applicables concernant les opérateurs d'importance vitale et leur résilience.

4.2. IMPACTS ECONOMIQUES ET FINANCIERS

4.2.1. Impacts macroéconomiques

Les mesures de résilience prévues pourront engendrer des coûts supplémentaires pour un opérateur. Si la logique de protection physique était déjà prise en compte, la systématisation de la prise en compte de la continuité d'activité ne sera en effet pas neutre. Ces coûts sont extrêmement difficiles à évaluer tant les opérateurs de la SAIV opèrent dans des secteurs diversifiés et à différentes échelles.

Néanmoins, le principe de résilience – au cœur de cette transposition – permettra *in fine* à l'opérateur et – au regard de certaines dépendances – à l'ensemble du tissu économique de pouvoir maintenir son activité dans un contexte dégradé et vise à amortir les coûts imputables à la disruption de son activité.

4.2.2. Impacts sur les entreprises

Le nouveau dispositif n'entraîne pas de changement majeur quant au mode de coopération des entreprises au sein du dispositif de sécurité des activités d'importance vitale. Ce dernier continuera de s'effectuer à leurs frais. Le coût global restera semblable à celui correspondant au dispositif actuellement en vigueur, qui contenait déjà des obligations de protection physique, mais aussi de continuité d'activité (article L. 2151-4 du code de la défense).

Le coût individuel du dispositif pour chaque opérateur est difficilement quantifiable, car celui-ci est fonction d'un nombre important de facteurs (taille de l'opérateur, allant de la TPE au grand groupe ; secteur d'activité concerné ; probabilité d'occurrence et gravité des risques identifiés). Par ailleurs, certains dispositifs déjà existant permettent des reconnaissances d'équivalence, n'induisant pas de surcoût pour les opérateurs (par exemple, le code ISPS pour la sureté portuaire). Enfin, ce dispositif est de nature à réduire les risques supportés en cas de disruption de l'activité.

4.2.3. Impacts budgétaires

L'impact est limité aux éventuels besoins en ressources humaines qui résulteront du renforcement du suivi du dispositif par les ministères et les échelons locaux en charge de superviser la SAIV. Enfin, ce dispositif est de nature à réduire les risques supportés en cas de disruption de l'activité.

4.3. IMPACTS SUR LES COLLECTIVITES TERRITORIALES

Les dispositions envisagées n'entraînent pas de frais supplémentaires pour les collectivités territoriales déjà concernées par le dispositif en vigueur, les obligations de protection et de continuité d'activité figurant déjà dans la loi. Certaines collectivités territoriales sont en effet déjà désignées en tant qu'OIV en raison des activités qu'elles assurent pour leurs administrés. En revanche, de nouvelles collectivités pourraient être concernées par le dispositif, dès lors qu'elles auraient à leur charge des opérateurs d'importance vitale figurant dans les nouveaux secteurs d'activité.

En revanche, les dispositions prévues dans le présent article permettront aux collectivités territoriales concernées par le dispositif d'être systématiquement informées que leur

délégataire exerce une activité d'importance vitale ou gère une infrastructure critique pour leur compte.

4.4. IMPACTS SUR LES SERVICES ADMINISTRATIFS

Comme dans le dispositif existant, les présentes mesures prévoient que la désignation des opérateurs d'importance vitale se fera par l'autorité administrative (ministère coordinateur ou préfet de département après avis de la CIDS ou de la CZDS).

4.5. IMPACTS SOCIAUX

4.5.1. Impacts sur la société

Le renforcement des exigences en matière de résilience des activités d'importance vitale doit permettre de limiter les impacts d'une crise ou de problèmes majeurs d'un opérateur d'importance vitale sur le fonctionnement de la société.

4.5.2. Impact sur les personnes en situation en handicap

Sans objet.

4.5.3. Impacts sur l'égalité entre les femmes et les hommes

Sans objet.

4.5.4. Impacts sur la jeunesse

Sans objet.

4.5.5. Impacts sur les professions réglementées

Sans objet.

4.6. IMPACTS SUR LES PARTICULIERS

Sans objet.

4.7. IMPACTS ENVIRONNEMENTAUX

Le dispositif conserve la catégorie spécifique des opérateurs industriels à haut-risque, notamment à des fins de protection de l'environnement. Certaines installations peuvent avoir des impacts (pollution de l'eau, de l'air, des sols, etc.) et présenter des dangers (incendie, explosion, etc.) pour l'environnement, la santé et la sécurité publique. Certains établissements classés ICPE peuvent donc être désignés OIV (voir schémas au 1.1.2 de ce chapitre).

L'objectif de ce dispositif est également, comme c'est le cas depuis 2013, de protéger les OIV face aux risques naturels (inondations, incendie, etc.)

5. CONSULTATIONS MENEES ET MODALITES D'APPLICATION

5.1. CONSULTATIONS MENEES

Une concertation de l'ensemble des ministères coordonnateurs a été réalisée sur cette mesure.

En application de l'article L. 1212-2 du code général des collectivités territoriales, le présent article a été soumis à l'examen du Conseil national d'évaluation des normes qui a rendu un avis défavorable le 22 mai 2024.

Enfin, le service national des enquêtes administratives de sécurité, le coordinateur général de la sécurité nucléaire, le service juridique du Secrétariat général des affaires européennes et l'Agence nationale de sécurité des systèmes d'informations ont également été consultés.

5.2. MODALITES D'APPLICATION

5.2.1. Application dans le temps

Les présentes dispositions entrent en vigueur le lendemain de la publication de la loi au *Journal officiel* de la République française.

Les opérateurs d'importance vitale désignés avant l'entrée en vigueur des dispositions du titre I^{er} de la présente loi doivent être regardés comme désignés en application du I de l'article L. 1332-2 du code de la défense dans sa rédaction résultant du chapitre I^{er} de la loi à la date de son entrée en vigueur.

Ces opérateurs restent soumis aux obligations qui leurs sont applicables avant l'entrée en vigueur de la présente loi jusqu'à l'accomplissement des obligations prévues aux articles L. 1332-2 à L. 1332-5 et à l'article L. 1332-11 dans leur rédaction résultant de la présente loi.

5.2.2. Application dans l'espace

Le présent article est applicable de plein droit sur l'ensemble du territoire de la République conformément à l'article L. 1 du code de la défense.

Aussi, les dispositions du code de la défense créées par le présent projet de loi seront applicables de plein droit à la fois dans les collectivités régies par le principe de l'identité législative (la Guadeloupe, la Guyane, la Martinique, La Réunion, Mayotte, Saint-Barthélemy, Saint-Martin et Saint-Pierre-et-Miquelon) et par le principe de la spécialité législative (les îles Wallis et Futuna, la Polynésie française, la Nouvelle-Calédonie et les Terres australes et antarctiques françaises).

Les nouveaux articles L. 1332-2 et L. 1332-3 du code de la défense renvoient à des dispositions du code de l'environnement qui ne sont pas applicables à Saint-Barthélemy, dans les îles Wallis et Futuna, en Polynésie française, en Nouvelle-Calédonie et dans les Terres australes et antarctiques françaises, les collectivités étant compétentes dans cette matière. Si l'article L. 6311-1 du code de la défense prévoit déjà une grille de lecture générale qui couvre toute la partie législative pour son application dans les îles Wallis et Futuna, en Polynésie française, en Nouvelle-Calédonie et dans les Terres australes et antarctiques françaises, il n'existe de grille similaire pour Saint-Barthélemy. Il est proposé de créer une grille sur le même modèle au sein d'un nouvel article L. 6221-2 du code de la défense, par l'article 3 du présent projet de loi.

Par ailleurs, en tant que PTOM, le droit de l'union européenne ne s'applique pas à Saint-Barthélemy, Saint-Pierre-et-Miquelon, dans les îles Wallis et Futuna, en Polynésie française, Nouvelle-Calédonie et dans les Terres australes et antarctiques françaises. Les dispositions applicables aux seuls OIV exerçant des services essentiels au fonctionnement du marché intérieur de l'Union européenne ne seront donc pas applicables en l'absence d'adaptation.

5.2.3. Textes d'application

Le présent article fera l'objet d'un décret en Conseil d'Etat pour préciser notamment les conditions des désignations des opérateurs par l'autorité administrative compétente.

Article 1er (C) – Article L. 1332-3 du code de la défense – Obligation de résilience

6. ETAT DES LIEUX

6.1. CADRE GENERAL

Le dispositif de la sécurité des activités d'importance vitale (SAIV) repose aujourd'hui sur une logique de protection *via* une obligation de résultats et non de moyens. Il s'agit d'une politique publique par laquelle l'opérateur doit démontrer auprès de l'autorité administrative la sécurisation de ses sites. Cette démonstration s'effectue par la planification qu'il doit mettre en œuvre, validée par l'administration.

Réalisation par l'opérateur d'une analyse des risques et des menaces

Une fois l'opérateur d'importance vitale désigné par la Commission interministérielle de défense et de sécurité (CIDS), celui-ci se voit notifier une ou plusieurs Directives Nationales de Sécurité (DNS), selon le ou les secteurs d'activité dans lequel il opère. La Directive nationale de sécurité permet à l'opérateur d'identifier les risques et les menaces contre lesquels il doit se prémunir en totalité ou en partie. Charge à lui, sur la base de cette analyse des risques générale au niveau du secteur d'activité, de réaliser sa propre analyse, au niveau de l'opérateur lui-même, ainsi que de ses sites.

Réalisation par l'opérateur du plan de sécurité d'opérateur (PSO)

Contrairement au plan particulier de protection qui est clairement identifié dans la partie législative du code de la défense, le plan de sécurité opérateur (PSO) n'est aujourd'hui évoqué que dans la partie réglementaire de celui-ci (articles R. 1332-19, R. 1332-20, R. 1332-21 et R. 1332-22).

Le PSO définit la politique et l'organisation de la sécurité de l'opérateur. Cette politique peut s'appuyer sur le dispositif de sécurité existant et sur l'expérience acquise dans la gestion de la qualité. Il précise, de façon générique, certaines des mesures à mettre en œuvre pour chaque point d'importance vitale (PIV) tant sur le plan organisationnel (organiser l'alerte et gérer la crise), qu'en matière de prévention (réduire les vulnérabilités) et de protection (réduire les conséquences). Il n'est requis que si l'opérateur gère plusieurs points d'importance vitale (PIV).

Il est fondé sur une analyse de risque prenant en compte notamment les scénarios de la ou les directives nationales de sécurité (DNS). Le PSO doit permettre à l'opérateur de s'approprier la DNS à travers la rédaction d'une analyse de risque propre à l'OIV. Il permet à l'opérateur

de s'interroger sur des scénarios majeurs et, le cas échéant, de repenser certains dispositifs opérationnels. Il doit également amener à une connaissance partagée de ces enjeux avec les pouvoirs publics. Il prévoit des mesures permanentes et graduées transposant tant les mesures spécifiques des DNS que les mesures Vigipirate applicables (voir partie *infra*). Le PSO prévoit s'il y a lieu, les délais de réalisation des mesures de protection permanentes et des mesures temporaires et graduées qu'il prescrit. En plus de l'identification et la mise en place des mesures, l'opérateur identifie dans son plan de sécurité opérateur les points d'importance vitale (PIV) sans lesquels il ne peut assurer l'activité d'importance vitale pour la ou lesquelles il a été désigné.

La sélection des PIV proposés par l'opérateur est issue de l'analyse de risque qui explicite les raisons pour lesquelles chaque point est proposé. La liste des PIV précise succinctement la nature de l'activité qui s'exerce pour chacun des points. Dans le cas où le PSO est élaboré à partir de plusieurs directives, la liste des PIV qui lui est annexée précise pour chaque PIV la ou les directive(s) qui s'y applique(nt). Dans le cas où l'opérateur envisage de proposer un seul établissement, un seul ouvrage ou une seule installation comme PIV, il accuse réception de la DNS qui lui a été transmise et soumet au ministère coordonnateur, dans un délai de six mois à compter de la date de notification de la DNS qui lui est applicable, une analyse de risque justifiant *in fine* la désignation d'un unique PIV. Il précise à cette occasion les caractéristiques géographiques et économiques du PIV. Dans le cas où l'opérateur envisage de proposer la désignation de plusieurs PIV, l'opérateur dispose d'un délai de six mois à compter de la date de notification de la dernière DNS qui lui est applicable pour soumettre une première version de son PSO au ministre coordonnateur. Si l'OIV ressent le besoin de se voir communiquer, à titre d'information, une autre DNS, il en formule une demande motivée auprès de l'autorité l'ayant désigné OIV. Celle-ci transmet la demande au ministre coordonnateur en charge de cette directive avec son avis sur la suite à réserver à cette demande.

Elaboration du plan de sécurité opérateur

Une fois désigné par l'autorité administrative, un OIV se voit communiquer le guide d'élaboration et le plan-type du PSO à l'occasion de la notification de la ou des DNS de son secteur d'activité. Le plan type actuel du PSO est fixé par l'arrêté du 2 juillet 2018 portant approbation du plan type des plans de sécurité d'opérateurs d'importance vitale. L'opérateur doit se conformer au plan type définit par arrêté du Premier ministre. Comme vu *infra*, l'opérateur dispose de six mois pour soumettre la première version de son plan de sécurité opérateur au ministère coordonnateur lui ayant notifié sa directive nationale de sécurité. Ce travail doit être effectué par une personne appartenant à l'organisation de l'OIV habilitée au secret de la défense nationale, condition obligatoire étant donné que les directives nationales de sécurité, essentielles pour rédiger le PSO, sont classifiées (en raison de la sensibilité de la partie portant sur les menaces). Dès que le ministère établit que le plan de sécurité opérateur est satisfaisant, il propose sa validation en commission interministérielle de défense et de

sécurité (CIDS) ou en Commission zonale de défense et de sécurité si l'opérateur ne se situe que sur une zone de défense et de sécurité. En application de l'article R-1332-18 du code de la défense, cette commission s'assure que :

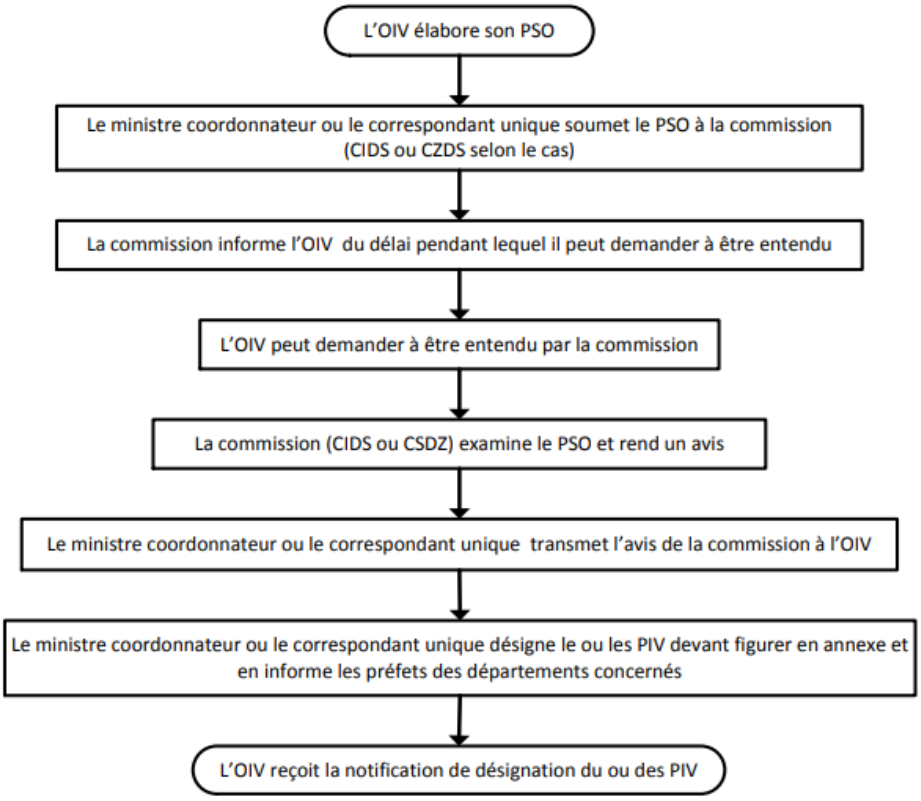
- les mesures proposées répondent de manière satisfaisante aux directives nationales de sécurité ;
- la liste des points d'importance vitale est pertinente ;
- la politique générale de sécurité définit des mesures spécifiques graduées de vigilance, de prévention, de protection et de réaction à une menace.

D'après l'article R 1332-21 du code de la défense, la commission émet dans un délai de trois mois à compter de la date de réception du plan un avis qui est notifié à l'opérateur. Cet avis est protégé par le secret de la défense nationale à l'instar du plan de sécurité opérateur une fois validés sont protégés par le secret de la défense nationale.

Une fois le plan de sécurité opérateur validé, l'opérateur est tenu de le mettre en œuvre, en lien avec le délégué à la défense et à la sécurité. Il est décliné ensuite pour chaque PIV sous la forme de plan particulier de protection. Pour les autres installations et réseaux de l'opérateur, il peut être décliné sous forme de directives, consignes particulières ou fiches réflexes, qui ne sont pas nécessairement classifiées. La politique d'exercices et d'audits concourt à l'évaluation du plan, en vue de son adaptation et de son amélioration.

Le PSO est aujourd'hui le fondement d'une politique générale de sécurité. Ce document de planification est indissociable d'une politique globale de gestion des risques.

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



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

Articulation avec les plans et réglementations existants

- *Le plan VIGIPIRATE*

Le plan VIGIPIRATE est le seul plan national dont la mise en œuvre est permanente. C'est un dispositif global de vigilance, de prévention et de protection qui concerne l'ensemble des secteurs d'activité du pays. Il implique tous les ministères, mais également l'ensemble de la population.

Le plan VIGIPIRATE repose sur trois piliers :

- le développement d'une culture de la sécurité au sein de la société ;
- un système de niveaux qui renforce la capacité de réponse de l'Etat ;
- la mise en œuvre de nouvelles mesures renforçant l'action gouvernementale dans la lutte contre le terrorisme.

Du fait de son obligation de se prémunir contre la menace, l'opérateur est tenu de prendre en compte la posture ainsi que les mesures identifiées dans le plan VIGIPIRATE. Pour ce faire, l'opérateur décline et adapte dans son PSO les mesures sectorielles et les mesures des domaines transverses du plan VIGIPIRATE qui lui sont applicables et qu'il est susceptible de mettre en œuvre pour atteindre les objectifs de sécurité fixés par la DNS. En effet, la DNS notifiée à l'opérateur précise les mesures du plan VIGIPIRATE applicables au secteur ou sous-secteur pour lequel il opère une activité d'importance vitale. Le PSO décline ces mesures qui doivent être classées en :

- mesures socle, correspondant aux investissements indispensables et aux actions permanentes de vigilance ;
- mesures additionnelles activables en fonction des consignes transmises à l'opérateur dans le cadre de l'activation de mesures spécifiques du plan VIGIPIRATE. Ces mesures peuvent être techniques, organisationnelles ou comportementales.

Les mesures du plan VIGIPIRATE, volontairement larges, doivent être adaptées et déclinées au contexte de l'entreprise. C'est l'objet du plan de sécurité opérateur (PSO) et du plan particulier de protection (PPP). Le PSO permet une forte collaboration entre l'État et l'ensemble des opérateurs désignés d'importance vitale afin de prendre des dispositions cohérentes avec celles que l'autorité administrative aura arrêtées ou recommandées au niveau national.

Afin de pouvoir mettre en œuvre les postures Vigipirate et être tenus informés de l'état de la menace, les opérateurs d'importance vitale sont destinataires des postures révisées. Les postures sont revues *a minima* tous les six mois et en cas d'évolution majeure de la menace.

- *Le plan de continuité d'activité (PCA)*

Le PCA décrit la stratégie adoptée par une organisation pour rétablir et reprendre son activité à la suite d'une perturbation importante. En listant et hiérarchisant l'ensemble des scénarios de risque et de menace pour un secteur donné, la directive nationale de sécurité constitue un référentiel pour le PCA et le PSO. Si ce dernier insiste sur les actes de malveillance (terrorisme, sabotage etc.), le PCA doit tenir compte de l'ensemble des scénarios.

Les OIV sont déjà tenus de rédiger un plan de continuité d'activité (article L. 2151-4 du code de la défense). Cette partie du code de la défense, qui régit le service de sécurité nationale (articles L. 2151-1 à L. 2151-5 du code de la défense), est destinée à « assurer la continuité de l'Etat, des collectivités territoriales, et des organismes qui leur sont rattachés, ainsi que des entreprises et établissements dont les activités contribuent à la sécurité nationale ». Elle concerne directement et uniquement les ouvrages désignés par les articles L. 1332-1 et L. 1332-2 du code de la défense, donc les OIV. Bien que cette partie du code de la défense ne soit pas celle normalement dédiée aux OIV, elle oblige bien les opérateurs désignés comme tels à réaliser des plans de continuité d'activité ou de rétablissement d'activité et surtout à

identifier les personnels considérés comme essentiels pour leur activité d'importance vitale (article L. 2151-1). Les personnes concernées par ces plans peuvent, en cas de déclenchement du service de sécurité nationale, être « maintenues dans leur emploi habituel ou tenues de le rejoindre » (article L. 2151-3).

Les opérateurs d'importance vitale sont donc bien tenus, dans la législation actuelle, de réaliser des plans de continuité d'activité. Ils ont la possibilité de le décliner pour chacun de leur PIV. Il est recommandé pour l'élaboration de ce plan de continuité d'activité, d'utiliser le guide méthodologique proposé par le secrétariat général de la défense et de la sécurité nationale (SGDSN) intitulé « Guide pour réaliser un plan de continuité d'activité »[19]. Toutefois, ce plan, contrairement aux autres plans actuellement existants (plan de sécurité opérateur, plan particulier de protection…) n'est aujourd'hui visé et validé par aucune autorité administrative. Il est donc bien censé exister, mais cela n'est vérifié de manière systématique par l'autorité administrative. Dans les faits, beaucoup d'opérateurs réalisent ou ont réalisé leur plan de continuité d'activité depuis la pandémie du Covid-19, qui a obligé beaucoup d'acteurs, qu'ils soient opérateurs ou non, à repenser leur organisation, y compris salariale en période de crise.

Délai et révision

Comme évoqué *supra*, le plan de sécurité opérateur (PSO) doit être réalisé par l'opérateur dans les six mois qui suivent la notification de la DNS.

La révision d'un PSO intervient en cas de modification d'une DNS, de changement d'activité de l'opérateur, ou encore en cas de modification majeure de son organisation ou de sa politique de sécurité.

Le plan particulier de protection (PPP) qui en découle doit lui être réalisé dans les deux ans à compter de la notification de la DNS. Une révision peut intervenir notamment à la suite d'un contrôle portant sur la mise en œuvre du plan ou à l'initiative de l'opérateur.

Pour le cas particulier de révision d'une DNS, l'article R. 1332-31 du code de la défense indique que la révision d'une DNS entraine la révision, dans les délais prévus pour leur élaboration, du PSO ainsi que des plans particuliers de protection concernés – cf. explication du nouvel article L. 1332-5 sur la planification que l'opérateur doit mettre en œuvre pour les sites qu'il identifie comme sensibles. Néanmoins, les modalités exactes de la révision du PSO et des PPP sont définies par le ministre coordonnateur en concertation avec l'OIV.

En résumé, dans le cadre actuel, l'opérateur doit élaborer :

[19] https://www.sgdsn.gouv.fr/files/files/Nos_missions/guide-pca-sgdsn-110613-normal.pdf.

- un Plan de Sécurité Opérateur dans le cas où il opère au moyen de plusieurs sites ou points d'importance vitale ;
- un Plan Particulier de Protection pour chaque point d'importance vitale (ce plan peut contenir une analyse du risque si l'opérateur n'a qu'un seul point d'importance vitale) ;
- éventuellement un PPP de zone d'importance vitale.

6.2. CADRE CONSTITUTIONNEL

Aux termes de l'article 88-1 de la Constitution : « La République participe aux Communautés européennes et à l'Union européenne, constituées d'Etats qui ont choisi librement, en vertu des traités qui les ont instituées, d'exercer en commun certaines de leurs compétences ». Le Conseil constitutionnel déduit de cette disposition que : « la transposition en droit interne d'une directive communautaire résulte d'une exigence constitutionnelle »[20]. Il en va de même pour une loi ayant pour objet d'adapter le droit interne à un règlement de l'Union européenne[21].

Les obligations d'analyse des risques et de mise en place d'un PSO-PRO à la charge des OIV, dont le manquement pouvant être sanctionné au niveau administratif, portent une atteinte à la liberté d'entreprendre, laquelle découle de l'article 4 de la Déclaration des droits de l'Homme et du Citoyen de 1789[22]. Cette atteinte ne peut être ni générale ni absolue[23]. Le législateur peut limiter l'exercice de cette liberté à la condition qu'il n'en résulte pas d'atteintes disproportionnées au regard de l'objectif poursuivi[24], alors même que cette atteinte résulterait de l'exigence constitutionnelle de transposition adéquate des directives européennes[25], dans un objectif de sécurité et de défense de la Nation, en l'absence de disposition spécifique contraire de la Constitution[26] ou de mise en cause d'une règle ou d'un principe inhérent à notre identité constitutionnelle[27].

[20] Voir notamment la décision n° 2004-496 DC du 10 juin 2004, « Loi pour la confiance dans l'économie numérique ».

[21] Voir par exemple la décision n° 2018-765, « Loi relative à la protection des données personnelles », considérant 3.

[22] Conseil constitutionnel, décision 98-401 DC du 10 juin 1998.

[23] Décision 82-141 DC du 27 juillet 1982.

[24] Décision 2023-1055 QPC du 16 juin 2023.

[25] Décision 2006-535 DC du 30 mars 2006.

[26] Décision 2004-497 DC du 1er juillet 2004.

[27] Décision 2018-765 DC du 12 juin 2018 ; décision 2019-818 QPC du 6 décembre 2019.

Enfin, en l'absence de remise en cause de ses garanties fondamentales, la liberté du commerce et de l'industrie ne s'oppose pas à l'intervention du législateur dans ce domaine[28].

6.3. CADRE CONVENTIONNEL

Au niveau européen, la directive (UE) 2022/2557 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience des entités critiques (REC) permet désormais d'offrir un socle minimal commun de résilience à tous les opérateurs de l'UE. Elle doit être transposée dans notre droit national d'ici le 17 octobre 2024.

Son champ d'application couvre 11 secteurs : énergie, transports, infrastructures bancaires, infrastructures de marché financier, santé, eau potable, assainissement, infrastructures digitales, administration publique (niveau central), espace, alimentation.

Son article 12 porte sur l'évaluation des risques par les entités critiques, et son article 13 sur les mesures de résilience des entités critiques.

6.4. ELEMENTS DE DROIT COMPARE

Sans objet.

7. NECESSITE DE LEGIFERER ET OBJECTIFS POURSUIVIS

7.1. NECESSITE DE LEGIFERER

L'article 34 de la Constitution qui prévoit que « *la loi détermine les principes fondamentaux (...) de la libre administration des collectivités territoriales, de leurs compétences et de leurs ressources* », témoignant de la nécessité de légiférer dans le présent cas lorsqu'une collectivité territoriale est concernée. Par ailleurs, une loi est nécessaire s'agissant de dispositions ayant nécessairement un impact sur la liberté d'entreprendre et la liberté du commerce et de l'industrie.

La nécessité de légiférer procède en outre de la transposition de la directive européenne sur la résilience des entités critiques (REC) du 14 décembre 2022.

En premier lieu, l'article 12 de la directive dispose que l'opérateur doit réaliser une évaluation des risques dans les neuf mois suivant la réception de la notification désignant l'opérateur comme entité critique, puis selon les besoins par la suite, et au moins tous les quatre ans, sur

[28] Décision 2003-474 DC du 17 juillet 2003.

la base des évaluations des risques d'Etats membres et d'autres sources d'informations pertinentes. Ces évaluations des risques doivent prendre en compte les risques naturels ainsi que les risques ayant une origine humaine. Il apparait donc indispensable de mentionner cette notion d'évaluation des risques à réaliser par les opérateurs dans la loi.

Par ailleurs, afin de répondre aux risques identifiés, l'article 13 de la directive impose la réalisation par les opérateurs désignés comme critiques par l'Etat membre d'un plan de résilience opérateur (PRO). L'interprétation à donner à cet article figure dans les considérants 30 et 31 de la directive REC, qui entérine le passage d'une logique de protection d'infrastructures critiques physiques, qui existait auparavant dans le dispositif de la SAIV à une logique de résilience des entités critiques. A ce jour, la partie législative du dispositif national de la SAIV comporte uniquement une obligation pour l'opérateur de réaliser les plans particuliers de protection (PPP) des sites qu'il a identifiés comme étant les plus sensibles, tandis que la réalisation du plan de sécurité opérateur s'appuie exclusivement sur des normes de niveau règlementaire. La consécration dans la loi de l'obligation pour les opérateurs de produire un plan de résilience opérateur (PRO) permettrait de clarifier les responsabilités respectives, en facilitant les échanges menés par les services de l'Etat auprès de l'opérateur désigné. Les opérateurs doivent réaliser et appliquer un plan de résilience qui permet de décrire les mesures prises par l'opérateur afin d'assurer la continuité du service essentiel pour lequel il a été désigné. Les autorités compétentes peuvent décréter que des plans ou des mesures mises en œuvre par les opérateurs désignés en vertu d'autres obligations juridiques de résilience et de sécurité peuvent être utilisées comme équivalent par ces derniers.

Etant donné que la politique publique de la SAIV est avant tout une politique de planification mise en œuvre par les opérateurs désignés par les autorités administratives compétentes, il apparait indispensable de pouvoir disposer d'une base législative permettant de fixer les délais pour la production et la révision du PRO, en garantissant la cohérence d'ensemble du dispositif, le cas échéant en appliquant des sanctions à l'OIV qui ne serait pas en capacité de se mettre en conformité avec les exigences fixées par la loi.

Les PRO contribueront à la préparation de l'opérateur, mais aussi de l'Etat, en cas de crise. Par comparaison, les plans de protection externe réalisés par l'autorité administrative en cas d'incident majeur malveillant sur un point d'importance vitale sont d'ailleurs faits en parfaite synergie avec les plans de l'opérateur.

7.2. OBJECTIFS POURSUIVIS

Clarification et consolidations des acquis du dispositif

L'objectif du projet de loi est de conserver les acquis et réalisations du dispositif de sécurité des activités d'importance vitale (SAIV). Depuis 2006, ce dispositif a exigé un important

travail de la part des opérateurs d'importance vitale désignés et des autorités administratives en charge du suivi.

Intégration de la notion de continuité d'activité et de résilience pour les opérateurs

L'objectif du projet de loi est également de renforcer la prise en compte de la composante « continuité d'activité » par les opérateurs.

A ce jour, seuls les PSO et les PPP, qui sont produits par l'opérateur, sont validés par l'autorité administrative. La commission interministérielle de défense et de sécurité (CIDS) valide les PSO – ou la Commission zonale de défense et de sécurité pour les opérateurs qui ne sont présents que sur une zone de défense et de sécurité. Les préfectures valident quant à elles les PPP, pour les PIV se situant sur leur territoire. En revanche, les plans de continuité d'activité (PCA) ne font pas l'objet d'une validation par l'autorité administrative, qui se contente de vérifier leur existence.

Ainsi, avec la fusion des actuels PSO et PCA pour devenir le PRO, l'objectif est d'améliorer la prise en compte de la continuité d'activité par les opérateurs, dans la mesure où ce dernier fera, comme le PSO, l'objet d'une validation de l'autorité administrative. L'autorité administrative devra donc valider si la politique générale de sécurité de l'opérateur est pertinente, mais également si les mesures de résilience préconisées par cet opérateur répondent aux exigences de continuité d'activité qu'imposent la directive REC.

Parallèlement, l'objectif est également de mieux distinguer les éléments classifiés de ce plan, sur le modèle des postures VIGIPIRATE : certaines dispositions sont classifiées, alors que d'autres, les plus sensibles, ne le sont pas. Cette distinction entre le classifié et le non-classifié fera l'objet d'une précision par voie réglementaire.

8. OPTIONS ENVISAGEES ET DISPOSITIF RETENU

8.1. OPTIONS ENVISAGEES

La première option à avoir été envisagée fut de conserver le dispositif actuel. Ainsi, la variété des plans existants aurait pu être maintenue. Le plan de continuité d'activité (PCA) serait resté un document annexe, décrit dans l'article L. 2151-4 du code de la défense. Le plan de sécurité opérateur (PSO) aurait également continué à être réalisé à part. Cette option a finalement été écartée, l'unification des deux plans en un document unique paraissant plus pertinente et simplificatrice pour les opérateurs, notamment au regard des obligations induites par la directive.

Une seconde option envisagée consistait à intégrer le plan de continuité d'activité au sein du plan particulier de protection (PPP). Ainsi, la stratégie de continuité d'activité aurait été

déployée à l'échelle de chaque point d'importance vitale (PIV) plutôt qu'au niveau global qui est le niveau du plan de sécurité opérateur (PSO). Il aurait donc été question de préciser le PPP, en lui ajoutant un volet relatif à la continuité d'activité. Cette option a elle aussi été écartée, le niveau de l'opérateur paraissant plus pertinent par les différents ministères coordonnateurs. La logique poursuivie était que, si un site désigné comme point d'importance vitale venait à ne plus fonctionner, l'opérateur pourrait se reposer sur d'autres sites d'importance vitale à partir desquels il réalise les activités pour lesquelles il a été désigné. Notamment, le nombre de démarches induites a été considéré trop élevé, dans le cas où cette option aurait été retenue, ce qui aurait fortement alourdi le travail des autorités administratives – qui sont les préfectures ou les délégués militaires départementaux pour les activités militaires de l'Etat – comme des opérateurs. Toutefois, il a été évoqué une possibilité de dérogation à cette règle, à savoir que dans certains cas la partie continuité d'activité soit réalisée dans les plans particuliers de protection (PPP), de manière à ce que les mesures de résilience puissent être mises en œuvre, le cas échéant et lorsque cela apparaît pertinent, au niveau des PIV. Cela paraissait important notamment pour les opérateurs qui étaient désignés via un site unique et afin de répondre aux particularités des différents secteurs d'activités concernés par la SAIV.

8.2. DISPOSITIF RETENU

Au regard du fonctionnement du dispositif existant, les travaux interministériels ont retenu l'option de fusionner le plan de sécurité opérateur (PSO) et le plan de continuité d'activité (PCA) en un plan de résilience opérateur (PRO) unique.

L'enjeu pour cet article est de conserver toute la spécificité du dispositif SAIV français, à savoir la planification comme moyen de démonstration avec le recours aux plans-type, qui ne seront pas forcément contraignants afin de laisser l'opérateur adapter le plan type à sa situation, son analyse de risque et l'évaluation des menaces réalisée par l'Etat. De même, la centralisation et la synthèse de la planification induite par le PRO apparait de nature à éviter les redondances présentes dans les différents dispositifs actuels.

Les deux premiers paragraphes de l'article permettent d'intégrer dans la loi l'obligation pour l'opérateur de réaliser une analyse des risques. Ce point permet de compléter les dispositions antérieures de l'article L. 1332-1 qui indiquaient que les établissements, installations et ouvrages des opérateurs identifiés comme point d'importance vitale devaient se protéger contre toute menace. La directive REC précise en effet que les opérateurs doivent prendre en compte les risques d'origine naturelle comme d'origine humaine – notion de « *all hazard approach* » de la directive.

Le troisième paragraphe précise les mesures que doivent mettre en œuvre les opérateurs pour assurer la notion de résilience, en conformité avec la définition figurant dans la directive.

Le terme de résilience est en effet la deuxième définition donnée à l'article 2 de la directive, à savoir « la capacité d'une entité critique à prévenir tout incident, à s'en protéger, à y réagir, à y résister, à l'atténuer, à l'absorber, à s'y adapter, et à s'en rétablir ».

Les quatrième et cinquième alinéas entérinent donc l'obligation pour l'opérateur de réaliser un plan de résilience opérateur – obligation qui découle de l'application réglementaire du dispositif existant mais aussi de la directive. Dans une logique d'allégement et de simplification pour l'opérateur et l'administration, un alinéa porte sur le principe d'équivalences possibles entre le dispositif SAIV et d'autres dispositifs de sécurité et de sureté existants, ce point étant explicitement prévu par la directive. Ainsi, le présent article donne à l'opérateur d'importance vitale la possibilité de se servir d'un plan de continuité d'activité existant pour l'intégrer à son PRO dans la partie devant porter sur les obligations de résilience, sur validation du principe par l'autorité administrative qui aurait vérifié que le plan en question répond aux exigences du dispositif SAIV.

Pour ce faire, il est également question de mieux distinguer les éléments classifiés au sein du plan : certaines parties, moins sensibles et utilisées dans le plan de continuité d'activité existant, pourraient donc être utilisées dans le plan de résilience opérateur. Ces informations provenant de documents non classifiés n'auraient donc pas vocation à l'être dans le plan de résilience opérateur, d'où le besoin de sections non classifiées dans le document. Dans cette perspective, il est prévu dans cet article de renvoyer au pouvoir règlementaire le soin de préciser les contours de la protection du secret dans le PRO.

Trois alinéas traitent des mesures de police administrative et de la possibilité de mise en demeure de l'opérateur par l'autorité compétente. Notamment, la création d'une possibilité d'astreinte d'un montant maximal de 5000 € par jour de retard d'élaboration, de révision ou de mise en œuvre du PRO. Cette possibilité d'astreinte paraît proportionnée au regard des enjeux de sécurité et de résilience de la Nation. Par ailleurs, ce montant de 5000 € permet de donner la possibilité à l'autorité administrative compétente – et il s'agirait ici des ministères coordonnateurs qui sont en charge de revoir les plans de sécurité opérateur – de prendre des premières mesures de contrainte dans le cas où l'opérateur ne répondrait pas à ses obligations et n'adopterait pas les mesures identifiées comme essentielles pour assurer sa résilience. Cette décision permet de contraindre si besoin est un opérateur récalcitrant à réaliser sa planification.

Un alinéa précise les modalités d'application de ces dispositions pour les opérateurs désignés au titre du danger grave pour la population (installations classées pour la protection de l'environnement au titre I^{er} du livre V du code de l'environnement ; dispositions relatives aux installation nucléaires de base prévues au chapitre III du titre IX du livre V du même code). Pour ces opérateurs, les obligations qui doivent prévaloir sont celles de la mise en sûreté et en sécurité plutôt que de continuité d'activité.

Un décret en Conseil d'Etat précise les modalités d'application du présent article.

9. ANALYSE DES IMPACTS DES DISPOSITIONS ENVISAGEES

9.1. IMPACTS JURIDIQUES

9.1.1. Impact sur l'ordre juridique interne

Les dispositions envisagées remplacent l'article L. 1332-3 du code de la défense.

Il est proposé de faire figurer dans la loi l'obligation pour les OIV de produire et mettre à jour un plan de résilience opérateur (PRO) s'appuyant sur une analyse des risques validée par l'autorité administrative compétente.

Ces dispositions portent une atteinte à la liberté d'entreprendre et à la liberté du commerce et de l'industrie qui est proportionnée et en rapport avec l'objectif poursuivi se rattachant à la défense et à la sécurité nationale.

Par ailleurs, le remplacement des dispositions des actuels articles L. 1332-1 et L. 1332-2 du code de la défense implique d'en tirer les conséquences dans les dispositions de droit interne qui font référence, selon les cas, à certains établissements, installations ou ouvrages, relevant de l'article L. 1332-1 (actuel), lesquels correspondront aux infrastructures critiques des opérateurs d'importance vitale.

Cet impact ne se limite pas aux seuls établissements, installations, ouvrages mais peut également concerner les opérateurs eux-mêmes, lesquels seront désormais qualifiés par la loi d'opérateurs d'importance vitale qui seront distincts selon les modalités de désignation, au titre du 1° ou du 2° du I de l'article L. 1332-2.

Enfin, les modifications prévues s'agissant des documents de planification ont entraîné des impacts sur les dispositions internes y faisant référence.

Toutes ces modifications induites ont été regroupées au sein d'un article 2, qui procède intégralement aux modifications nécessaires. Ces dispositions n'ont par elles-mêmes aucun autre impact que celui de modifier des références textuelles.

9.1.2. Articulation avec le droit international et le droit de l'Union européenne

Les dispositions de la présente mesure s'inscrivent dans le champ de la transposition de la directive européenne sur la résilience des entités critiques (REC) du 14 décembre 2022, en particulier son article 12, relatif à l'évaluation des risques par les entités critiques, et son article 13, portant sur les mesures de résilience des entités critiques.

9.2. IMPACTS ECONOMIQUES ET FINANCIERS

9.2.1. Impacts macroéconomiques

Les mesures de résilience prévues pourront engendrer des coûts supplémentaires pour un opérateur. Si la logique de protection physique était déjà prise en compte, la systématisation de la prise en compte de la continuité d'activité ne sera en effet pas neutre. Ces coûts sont extrêmement difficiles à évaluer tant les opérateurs de la SAIV opèrent dans des secteurs diversifiés et à différentes échelles.

Néanmoins, le principe de résilience – au cœur de cette transposition – permettra *in fine* à l'opérateur et – au regard de certaines dépendances - à l'ensemble du tissu économique de pouvoir maintenir son activité dans un contexte dégradé et vise à amortir les coûts imputables à la disruption de son activité.

9.2.2. Impacts sur les entreprises

La mise en place du PRO n'entraine pas de changement majeur quant au mode de coopération avec les autorités administratives, qu'il s'agisse d'opérateurs privés ou publics. En effet, les opérateurs avaient déjà à réaliser au titre de la SAIV un plan de sécurité opérateur ainsi qu'un plan de continuité d'activité. La différence majeure repose sur le fait que les autorités administratives en charge de vérifier et valider les éléments de la planification devront dorénavant également vérifier les parties relevant de la continuité d'activité – ancien plan de continuité d'activité – dans leur plan de résilience opérateur.

Les opérateurs continueront, comme ils l'ont fait jusqu'à présent, à assumer à leurs frais les mesures indispensables à leur résilience et à la continuité de leurs activités, c'est pourquoi la logique de démonstration par la planification de la SAIV est conservée. Ils sont tenus de prouver, par les mesures qu'ils auront prévues en lien avec l'autorité administrative, que celles-ci suffisent pour assurer leur résilience, en adéquation avec leur environnement ainsi que leur secteur d'activité.

9.2.3. Impacts budgétaires

Des moyens humains supplémentaires pourraient être rendus nécessaires par la plus grande régularité des contrôles et la validation des PRO produits par les OIV, pour les ministères coordinateurs et les zones de défense et de sécurité et le SGDSN.

9.3. IMPACTS SUR LES COLLECTIVITES TERRITORIALES

La mise en place du PRO n'entraine pas de changement majeur quant au mode de coopération avec les autorités administratives, qu'il s'agisse d'opérateurs privés ou publics. En effet, les opérateurs – ici les collectivités territoriales – avaient déjà à réaliser au titre de la SAIV un

plan de sécurité opérateur ainsi qu'un plan de continuité d'activité. La différence majeure repose sur le fait que les autorités administratives en charge de vérifier et valider les éléments de la planification devront dorénavant également vérifier les parties relevant de la continuité d'activité – ancien plan de continuité d'activité – dans leur plan de résilience opérateur.

Les collectivités territoriales désignées comme opérateurs continueront, comme elles l'ont fait jusqu'à présent, à assumer à leurs frais les mesures indispensables à leur résilience et à la continuité de leurs activités. La logique de démonstration par la planification de la SAIV est conservée. Elles sont tenues de prouver, par les mesures qu'ils auront prévues en lien avec l'autorité administrative, que celles-ci suffisent pour assurer leur résilience, en adéquation avec leur environnement ainsi que leur secteur d'activité

9.4. IMPACTS SUR LES SERVICES ADMINISTRATIFS

La procédure de contrôle et de validation du PRO par l'autorité administrative est identique aux procédures d'ores et déjà existantes dans le dispositif national de la SAIV.

Ces contrôles s'effectuent actuellement à deux niveaux :

- le ministère coordinateur fait valider le plan de résilience opérateur durant la Commission interministérielle de défense et de sécurité (CIDS) présidée par le SGDSN ;
- la zone de défense et de sécurité (ZDS) fait valider les plans de résilience opérateur des OIV se trouvant uniquement sur leurs territoires durant les commissions zonale de défense et de sécurité (CZDS).

A l'avenir, les services administratifs compétents continueront à réviser les plans de résilience opérateur, en vérifiant également le volet résilience – entendre ici les anciens plans de continuité d'activité visés à l'article L. 2151-4 du code de la défense.

La différence majeure introduite par le présent projet de loi, qui sera précisée par décret en Conseil d'Etat, réside dans l'introduction d'un cycle de révision obligatoire du PRO tous les quatre ans. L'autorité administrative devra s'adapter en conséquence, soit en réorganisant ses priorités à effectifs constants, soit en recrutant le cas échéant des ETP supplémentaires.

9.5. IMPACTS SOCIAUX

9.5.1. Impacts sur la société

Le renforcement des exigences en matière de résilience des activités d'importance vitale doit permettre de limiter les impacts d'une crise ou de problèmes majeurs d'un opérateur d'importance vitale sur le fonctionnement de la société.

9.5.2. Impact sur les personnes en situation en handicap

Sans objet.

9.5.3. Impacts sur l'égalité entre les femmes et les hommes

Sans objet.

9.5.4. Impacts sur la jeunesse

Sans objet.

9.5.5. Impacts sur les professions réglementées

Sans objet.

9.6. IMPACTS SUR LES PARTICULIERS

Sans objet.

9.7. IMPACTS ENVIRONNEMENTAUX

Le dispositif conserve la catégorie spécifique des opérateurs industriels à haut-risque, notamment à des fins de protection de l'environnement. Certaines installations peuvent avoir des impacts (pollution de l'eau, de l'air, des sols, etc.) et présenter des dangers (incendie, explosion, etc.) pour l'environnement, la santé et la sécurité publique. Pour ces raisons, elles sont soumises à une autre réglementation : celle des installations classées pour la protection de l'environnement (ICPE). Certains établissements classés ICPE peuvent donc être désignés OIV (voir schémas au 1.1.2 de ce chapitre).

L'objectif de ce dispositif est également, comme c'est le cas depuis 2013, de protéger les OIV face aux risques naturels (inondations, incendie, etc.)

10. CONSULTATIONS MENEES ET MODALITES D'APPLICATION

10.1. CONSULTATIONS MENEES

Une concertation de l'ensemble des ministères coordonnateurs a été réalisée sur cette mesure.

En application de l'article L. 1212-2 du code général des collectivités territoriales, le présent article a été soumis à l'examen du Conseil national d'évaluation des normes qui a rendu un avis défavorable le 22 mai 2024.

Enfin, le service national des enquêtes administratives de sécurité, le coordinateur général de la sécurité nucléaire, le service juridique du Secrétariat général des affaires européennes et l'Agence nationale de sécurité des systèmes d'informations ont également été consultés.

10.2. MODALITES D'APPLICATION

10.2.1. Application dans le temps

Les présentes dispositions législatives entrent en vigueur le lendemain de la publication de la présente loi au *Journal officiel* de la République française.

Les opérateurs d'importance vitale désignés avant l'entrée en vigueur des dispositions du titre I^{er} de la présente loi doivent être regardés comme désignés en application du I de l'article L. 1332-2 du code de la défense dans sa rédaction résultant du chapitre I^{er} de la loi à la date de son entrée en vigueur.

Ces opérateurs restent soumis aux obligations qui leurs sont applicables avant l'entrée en vigueur de la présente loi jusqu'à l'accomplissement des obligations prévues aux articles L. 1332-2 à L. 1332-5 et à l'article L. 1332-11 dans leur rédaction résultant de la présente loi.

10.2.2. Application dans l'espace

Le présent article est applicable de plein droit sur l'ensemble du territoire de la République conformément à l'article L. 1 du code de la défense.

Aussi, les dispositions du code de la défense créées par le présent projet de loi seront applicables de plein droit à la fois dans les collectivités régies par le principe de l'identité législative (la Guadeloupe, la Guyane, la Martinique, La Réunion, Mayotte, Saint-Barthélemy, Saint-Martin et Saint-Pierre-et-Miquelon) et par le principe de la spécialité législative (les îles Wallis et Futuna, la Polynésie française, la Nouvelle-Calédonie et les Terres australes et antarctiques françaises).

Les nouveaux articles L. 1332-2 et L. 1332-3 du code de la défense renvoient à des dispositions du code de l'environnement qui ne sont pas applicables à Saint-Barthélemy, dans

les îles Wallis et Futuna, en Polynésie française, en Nouvelle-Calédonie et dans les Terres australes et antarctiques françaises, les collectivités étant compétentes dans cette matière. Si l'article L. 6311-1 du code de la défense prévoit déjà une grille de lecture générale qui couvre toute la partie législative pour son application dans les îles Wallis et Futuna, en Polynésie française, en Nouvelle-Calédonie et dans les Terres australes et antarctiques françaises, il n'existe de grille similaire pour Saint-Barthélemy. Il est proposé de créer une grille sur le même modèle au sein d'un nouvel article L. 6221-2 du code de la défense, par l'article 3 du présent projet de loi.

Par ailleurs, en tant que PTOM, le droit de l'union européenne ne s'applique pas à Saint-Barthélemy, Saint-Pierre-et-Miquelon, dans les îles Wallis et Futuna, en Polynésie française, Nouvelle-Calédonie et dans les Terres australes et antarctiques françaises. Les dispositions applicables aux seuls OIV exerçant des services essentiels au fonctionnement du marché intérieur de l'Union européenne ne seront donc pas applicables en l'absence d'adaptation.

10.2.3. Textes d'application

Le présent article fera l'objet d'un décret en Conseil d'Etat, qui précisera la nature des mesures de résilience pour chaque catégorie d'opérateur d'importance vitale mentionnée au I de l'article L. 1332-2 du présent projet de loi.

Article 1er (D) – Article L. 1332-4 du code de la défense – Analyse des dépendances

1. ETAT DES LIEUX

1.1. CADRE GENERAL

Aujourd'hui, les opérateurs d'importance vitale (OIV), dès qu'ils sont désignés comme tels, doivent appréhender leur dépendance potentielle avec des sous-traitants.

En effet, dans le cadre de son activité normale, un OIV peut avoir sous-traité ou externalisé une ou plusieurs fonctions concourant à la réalisation de l'activité d'importance vitale en question. Dans ce cas, il appartient à l'opérateur de prendre les dispositions nécessaires vis-à-vis de son sous-traitant ou de son fournisseur, notamment dans les spécifications du contrat les liant, pour que celui-ci concoure à la réalisation des objectifs de sécurité de l'opérateur.

Par ailleurs, les actuels plans de sécurité des opérateurs (PSO) doivent faire figurer un certain nombre de dépendances :

- Les « dépendances amont » envers d'autres systèmes (énergie, télécommunications…) doivent être prises en compte dans l'analyse globale de sécurité ;
- De la même manière, les dépendances aval (conséquences de l'arrêt de l'opérateur pour d'autres secteurs d'activités d'importance vitale) doivent être décrites ;
- Enfin, les aspects internationaux doivent également être considérés (dépendance envers d'autres pays).

Par exemple, un laboratoire pharmaceutique désigné OIV précisera, dans la mesure du possible, son niveau de dépendance en matières premières importées de l'étranger.

La description des interdépendances doit permettre à l'opérateur de s'assurer que ces vulnérabilités sont correctement identifiées et, au besoin, redondées. De la même façon, cette information permet aux pouvoirs publics d'identifier d'éventuels opérateurs qui répondraient aux critères d'un OIV.

La crise sanitaire du Covid-19 a souligné combien l'économie mondialisée reposait désormais sur des chaînes de valeurs diffuses et des processus de production extrêmement fragmentés, de la conception à la distribution. C'est ainsi que les chaînes d'approvisionnement sont elles-mêmes fortement divisées entraînant des interdépendances marquées entre nations et continents mais aussi entre secteurs d'activité. Cela correspond aux processus de régionalisation, de polarisation et de développement du commerce interbranches identifiés

depuis une quinzaine d'années par des organisations comme l'organisation mondiale du commerce.

Ces interdépendances signifient que toute perturbation de services essentiels, même initialement limitée à une entité ou un secteur, peut produire des effets en cascade plus larges, entraînant éventuellement une incidence négative à long terme et de grande ampleur sur la fourniture de services dans l'ensemble du marché intérieur. Les crises majeures, telles que la pandémie de COVID-19, ont mis en évidence la vulnérabilité de nos sociétés de plus en plus interdépendantes face à des risques à faible probabilité de survenance, mais à fort impact.

Ainsi, au pic de la pandémie de Covid-19, le retour de contrôles stricts aux frontières des Etats, y compris au sein de l'Union européenne, a entrainé de nombreuses perturbations quant à la poursuite de certaines activités et/ou la distribution tant de composants intermédiaires que de produits finis de toutes natures (alimentaire, informatique, automobile, médicament, etc.).

Le contexte géopolitique, géoéconomique et sanitaire mondial se caractérise désormais par une particulière instabilité. Des conflits locaux ont dorénavant une incidence mondiale, à l'instar de l'approvisionnement en céréales perturbé par la guerre en Ukraine et le minage de la Mer Noire, principal point de départ du blé ukrainien, ou encore du conflit entre Israël et le Hamas entraînant un regain de tensions dans une région capitale pour le flux mondial des marchandises (canal de Suez) ainsi qu'en témoignent les attaques directement dirigées sur des navires commerciaux en Mer rouge par les rebelles Houtis. Il est aussi possible de citer les menaces de manœuvres chinoises au large de Taïwan, pays dominant largement la production des semi-conducteurs (60% de la production mondiale et 90% des exemplaires les plus avancés technologiquement) devenus absolument indispensables à nos économies largement numérisées.

Les exemples sont nombreux de retard ou même de pénuries de certains produits ou denrées : ainsi, lors de la récente pandémie de COVID-19 qui a servi de mise en situation, accélérant par là-même une prise de conscience en la matière, la France a constaté sa dépendance à la production de paracétamol et à d'autres principes actifs médicamenteux, dont les productions françaises et même européennes ne suffisent plus à couvrir les besoins de la population.

Il faut aussi souligner l'impact possible de catastrophes naturelles et du changement climatique sur certaines activités, lesquelles pourraient dès lors devoir fonctionner de manière dégradée, voire même s'interrompre.

De manière générale, l'évolution vers plus d'imprévisibilité géopolitique mais aussi une diversification des menaces de toutes natures sur la scène internationale doit conduire les opérateurs d'importance vitale à intégrer davantage dans leur réflexion de protection leur propre évolution dans leur environnement d'activité et ce, au sens le plus large possible. Il ne s'agit donc plus de prendre seulement en compte la sécurité de leurs installations physiques

mais bel et bien de tous les éléments qui concourent même indirectement au fonctionnement nominal de leurs activités.

Les opérateurs du secteur privé disposent d'ores et déjà de cette habitude dans la mesure où la rentabilité économique de leurs activités dépend pour large partie de l'environnement global dans lequel elles se déploient. Un approvisionnement défaillant, une chaîne de valeur interrompue et donc une ligne de production par conséquent à l'arrêt sont autant d'éléments dont ces opérateurs doivent anticiper les effets pour éviter *in fine* une éventuelle défaillance.

1.2. CADRE CONSTITUTIONNEL

Aux termes de l'article 88-1 de la Constitution : « La République participe aux Communautés européennes et à l'Union européenne, constituées d'Etats qui ont choisi librement, en vertu des traités qui les ont instituées, d'exercer en commun certaines de leurs compétences ». Le Conseil constitutionnel déduit de cette disposition que : « la transposition en droit interne d'une directive communautaire résulte d'une exigence constitutionnelle »[29]. Il en va de même pour une loi ayant pour objet d'adapter le droit interne à un règlement de l'Union européenne[30].

Les obligations d'analyse de dépendance à la charge des OIV dont le manquement pouvant être sanctionné au niveau administratif, portent une atteinte à la liberté d'entreprendre, laquelle découle de l'article 4 de la Déclaration des droits de l'Homme et du Citoyen de 1789[31]. Cette atteinte ne peut être ni générale ni absolue[32]. Le législateur peut limiter l'exercice de cette liberté à la condition qu'il n'en résulte pas d'atteintes disproportionnées au regard de l'objectif poursuivi[33], alors même que cette atteinte résulterait de l'exigence constitutionnelle de transposition adéquate des directives européennes[34], dans un objectif de sécurité et de défense de la Nation, en l'absence de disposition spécifique contraire de la Constitution[35] ou de mise en cause d'une règle ou d'un principe inhérent à notre identité constitutionnelle[36].

[29] Voir notamment la décision n° 2004-496 DC du 10 juin 2004, « Loi pour la confiance dans l'économie numérique ».

[30] Voir par exemple la décision n° 2018-765, « Loi relative à la protection des données personnelles », considérant 3.

[31] Conseil constitutionnel, décision 98-401 DC du 10 juin 1998.

[32] Décision 82-141 DC du 27 juillet 1982.

[33] Décision 2023-1055 QPC du 16 juin 2023.

[34] Décision 2006-535 DC du 30 mars 2006.

[35] Décision 2004-497 DC du 1er juillet 2004.

[36] Décision 2018-765 DC du 12 juin 2018 ; décision 2019-818 QPC du 6 décembre 2019.

Enfin, en l'absence de remise en cause de ses garanties fondamentales, la liberté du commerce et de l'industrie ne s'oppose pas à l'intervention du législateur dans ce domaine[37].

1.3. CADRE CONVENTIONNEL

Au niveau européen, la directive (UE) 2022/2557 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience des entités critiques (REC) permet désormais d'offrir un socle minimal commun de résilience à tous les opérateurs de l'UE. Elle doit être transposée dans notre droit national d'ici le 17 octobre 2024.

Son champ d'application couvre 11 secteurs : énergie, transports, infrastructures bancaires, infrastructures de marché financier, santé, eau potable, assainissement, infrastructures digitales, administration publique (niveau central), espace, alimentation.

L'identification des dépendances par les opérateurs d'importance vitale est prévue par les articles 4, 12 et 19 de la directive UE 2022/2557 du Parlement européen et du Conseil du 14 décembre 2022.

1.4. ÉLEMENTS DE DROIT COMPARE

Sans objet.

2. NECESSITE DE LEGIFERER ET OBJECTIFS POURSUIVIS

2.1. NECESSITE DE LEGIFERER

L'application de l'article 34 de la Constitution impose l'adoption d'une disposition de nature législative, dès lors qu'elle peut être regardée comme déterminant un principe fondamental d'organisation de la défense nationale et qu'il s'agit d'une sujétion imposée aux opérateurs, ainsi qu'il a été rappelé précédemment.

Le deuxième paragraphe de l'article 12 de la directive européenne REC précise par ailleurs :

« Lorsqu'une entité critique a réalisé d'autres évaluations des risques ou établi des documents en vertu d'obligations prévues dans d'autres actes juridiques qui sont pertinents pour son évaluation des risques d'entité critique, elle peut utiliser ces évaluations et documents pour satisfaire aux exigences énoncées dans le présent article. Dans l'exercice de ses fonctions de supervision, l'autorité compétente peut déclarer qu'une évaluation des risques existante

[37] Décision 2003-474 DC du 17 juillet 2003.

réalisée par une entité critique qui porte sur les risques et le degré de dépendance visés au premier alinéa du présent paragraphe respecte, en tout ou en partie, les obligations prévues par le présent article ».

Il peut être également souligné à nouveau que ces sujétions, qui portent atteinte à la liberté d'entreprendre et à la liberté du commerce et de l'industrie, sont proportionnées à l'objectif qui s'attache à la défense et à la résilience de la Nation.

2.2. OBJECTIFS POURSUIVIS

Les dispositions envisagées visent à faire de l'analyse des dépendances une obligation en soit, et à exiger des opérateurs qu'ils en tirent les conséquences opérationnelles dans leur politique de résilience.

3. OPTIONS ENVISAGEES ET DISPOSITIF RETENU

3.1. OPTIONS ENVISAGEES

Cette analyse aurait pu être intégrée dans les dispositions relatives à l'analyse de risque, mais le choix a été fait d'isoler cette partie pour que les opérateurs effectuent un travail de recensement exhaustif de leurs dépendances, afin que le risque de rupture d'approvisionnement ne soit pas appréhendé comme un simple risque générique non détaillé.

3.2. DISPOSITIF RETENU

Les présentes dispositions créent une obligation pour les opérateurs de réaliser une analyse des risques de dépendance à l'égard de tous les acteurs, nationaux, européens ou internationaux, susceptibles d'être indispensables à la réalisation de leur activité d'importance vitale, quel que soit le positionnement occupé dans la phase d'activité et/ou de production de ce tiers. Cette étude comprend une analyse des vulnérabilités des chaines d'approvisionnement.

Pour donner une valeur réellement préventive et une nature positive à cette analyse des dépendances, les conclusions de cette analyse doivent faire l'objet de traductions concrètes dans les mesures nécessaires pour garantir l'application des dispositions

4. ANALYSE DES DISPOSITIONS ENVISAGEES

4.1. IMPACTS JURIDIQUES

4.1.1. Impact sur l'ordre juridique interne

La présente mesure remplace l'article L. 1332-4 du code de la défense au sein du chapitre II « résilience des activités d'importance vitale » (et non plus « protection des installations d'importance vitale »).

Ces dispositions portent une atteinte à la liberté d'entreprendre et à la liberté du commerce et de l'industrie qui est proportionnée et en rapport avec l'objectif poursuivi se rattachant à la défense et à la sécurité nationale.

4.1.2. Articulation avec le droit international et le droit de l'Union européenne

Les présentes dispositions du projet de loi permettent d'assurer la cohérence du droit français avec la réglementation européenne qui procède de la directive REC, notamment ses articles 4, 12 et 19, qui traitent de l'identification de leurs dépendances par les opérateurs d'importance vitale.

4.2. IMPACTS ECONOMIQUES ET FINANCIERS

4.2.1. Impacts macroéconomiques

La présente disposition, à travers le dispositif de recensement des dépendances qu'elle prévoit, permet d'accroître la résilience globale de l'économie. En effet, en identifiant toutes les dépendances et interdépendances des opérateurs d'importance vitale, quelle que soit la localisation ou le positionnement des sous-traitants dans le processus de production, il est possible d'anticiper une crise potentielle ayant une incidence sur l'un de ces sous-traitants et donc d'assurer la préparation d'une stratégie de poursuite d'activité, y compris économique.

4.2.2. Impacts sur les entreprises

Une telle mesure assure à l'outil de production des entreprises l'anticipation des risques, notamment les ruptures d'approvisionnement, et leur fournit donc les moyens d'assurer sa propre continuité de fonctionnement. Les entreprises désignées comme opérateurs continueront, comme elles l'ont fait jusqu'à présent, à assumer à leurs frais les mesures indispensables à leur résilience. La logique de démonstration par la planification de la SAIV est conservée. Les entreprises désignées comme opérateurs sont tenues de prouver, par les mesures qu'ils auront prévues en lien avec l'autorité administrative, que celles-ci suffisent pour assurer leur résilience, en adéquation avec leur environnement ainsi que leur secteur d'activité.

4.2.3. Impacts budgétaires

Sans objet.

4.3. IMPACTS SUR LES COLLECTIVITES TERRITORIALES

Les collectivités territoriales désignées comme opérateurs continueront, comme elles l'ont fait jusqu'à présent, à assumer à leurs frais les mesures indispensables à leur résilience, c'est pourquoi la logique de démonstration par la planification de la SAIV est conservée. Les collectivités territoriales désignées comme opérateurs sont tenues de prouver, par les mesures qu'ils auront prévues en lien avec l'autorité administrative, que celles-ci suffisent pour assurer leur résilience, en adéquation avec leur environnement ainsi que leur secteur d'activité.

4.4. IMPACTS SUR LES SERVICES ADMINISTRATIFS

Les administrations en charge de la validation des documents de planification (ministères coordonnateurs, zones de défense, préfectures de département) devront analyser le respect de ces obligations dans les documents transmis, ce qui constituera une charge de travail supplémentaire pouvant avoir des impacts sur les ressources humaines.

4.5. IMPACTS SOCIAUX

4.5.1. Impacts sur la société

Le renforcement des exigences en matière de résilience des activités d'importance vitale doit permettre de limiter les impacts d'une crise ou de problèmes majeurs d'un opérateur d'importance vitale sur le fonctionnement de la société.

4.5.2. Impact sur les personnes en situation en handicap

Sans objet.

4.5.3. Impacts sur l'égalité entre les femmes et les hommes

Sans objet.

4.5.4. Impacts sur la jeunesse

Sans objet.

4.5.5. Impacts sur les professions réglementées

Sans objet.

4.6. IMPACTS SUR LES PARTICULIERS

Sans objet.

4.7. IMPACTS ENVIRONNEMENTAUX

Sans objet.

5. CONSULTATIONS MENEES ET MODALITES D'APPLICATION

5.1. CONSULTATIONS MENEES

Une concertation de l'ensemble des ministères coordonnateurs a été réalisée sur cette mesure.

En application de l'article L. 1212-2 du code général des collectivités territoriales, le présent article a été soumis à l'examen du Conseil national d'évaluation des normes qui a rendu un avis défavorable le 22 mai 2024.

Enfin, le service national des enquêtes administratives de sécurité, le coordinateur général de la sécurité nucléaire, le service juridique du Secrétariat général des affaires européennes et l'Agence nationale de sécurité des systèmes d'informations ont également été consultés.

5.2. MODALITES D'APPLICATION

5.2.1. Application dans le temps

Les présentes dispositions entrent en vigueur le lendemain de la publication de la présente loi au *Journal officiel* de la République française.

Les opérateurs d'importance vitale désignés avant l'entrée en vigueur des dispositions du titre I^{er} de la présente loi doivent être regardés comme désignés en application du I de l'article L. 1332-2 du code de la défense dans sa rédaction résultant du chapitre I^{er} de la loi à la date de son entrée en vigueur.

Ces opérateurs restent soumis aux obligations qui leurs sont applicables avant l'entrée en vigueur de la présente loi jusqu'à l'accomplissement des obligations prévues aux articles L. 1332-2 à L. 1332-5 et à l'article L. 1332-11 dans leur rédaction résultant de la présente loi.

5.2.2. Application dans l'espace

Le présent article est applicable de plein droit sur l'ensemble du territoire de la République conformément à l'article L. 1 du code de la défense.

Aussi, les dispositions du code de la défense créées par le présent projet de loi seront applicables de plein droit à la fois dans les collectivités régies par le principe de l'identité législative (la Guadeloupe, la Guyane, la Martinique, La Réunion, Mayotte, Saint-Barthélemy, Saint-Martin et Saint-Pierre-et-Miquelon) et par le principe de la spécialité législative (les îles Wallis et Futuna, la Polynésie française, la Nouvelle-Calédonie et les Terres australes et antarctiques françaises).

En tant que PTOM, le droit de l'union européenne ne s'applique pas à Saint-Barthélemy, Saint-Pierre-et-Miquelon, dans les îles Wallis et Futuna, en Polynésie française, Nouvelle-Calédonie et dans les Terres australes et antarctiques françaises. Les dispositions applicables aux seuls OIV exerçant des services essentiels au fonctionnement du marché intérieur de l'Union européenne ne seront donc pas applicables en l'absence d'adaptation.

5.2.3. Textes d'application

Le présent article fera l'objet d'un décret en Conseil d'Etat afin de préciser les modalités d'élaboration de l'analyse des dépendances.

Article 1er (E) – Article L. 1332-5 du code de la défense – Plan Particulier de Résilience

1. ETAT DES LIEUX

1.1. CADRE GENERAL

Une fois désignés, les opérateurs d'importance vitale sont tenus de réaliser un Plan de sécurité d'opérateur (PSO) et identifient leurs points d'importance vitale (PIV). Ces derniers sont les établissements et ouvrages nécessaires à la réalisation des activités d'importance vitale et, sont désignés de manière formelle par un arrêté du ministère coordonnateur.

La protection des PIV repose sur deux types de plans :

- un plan particulier de protection (PPP), élaboré par l'opérateur et validé par l'autorité administrative, qui précise les mesures de protection internes prévues par l'opérateur ;
- un plan de protection externe (PPE) précise les mesures de protection externes planifiées de vigilance, de prévention, de protection et de réaction prévues par les pouvoirs publics. Ce deuxième plan est réalisé après validation par l'autorité administrative du plan particulier de protection et vise à organiser la réponse de l'Etat en cas d'incident majeur auquel le plan particulier de protection ne saurait répondre seul.

Ces deux plans sont classifiés au niveau secret et validés par arrêté préfectoral.

1.1.1. Plan particulier de protection (PPP)

Dans le dispositif actuel de sécurité des activités d'importance vitale, les articles L. 1332-3 à L. 1332-5 du code de la défense, ainsi que les articles R. 1332-15 et R. 1332-23 à R. 1332-32 du code de la défense, précisent les dispositions en vigueur concernant le plan particulier de protection.

L'objectif des mesures contenues dans ces plans est de mettre en échec ou à défaut, retarder les tentatives malveillantes, à en limiter les effets et à faciliter la continuité d'activité et le rétablissement d'activité. Certaines mesures sont mises en œuvre en permanence, d'autres de manière temporaire lorsque la nécessité s'en fait sentir ou sur décision du gouvernement ou de son représentant local (notamment dans le cadre du plan VIGIPIRATE).

Les PPP sont des outils essentiels de la SAIV dans la mesure où ils démontrent les mesures de protection prises par l'opérateur, répondant à une logique de résultats (et non de moyens) dans le cadre d'une relation de partenariat avec l'Etat.

Elaboration du plan particulier de protection (PPP)

L'opérateur élabore le PPP du PIV concerné, dans un délai de deux ans à compter de la notification de la dernière Directive nationale de sécurité (DNS) qui lui est applicable. Pour son élaboration, il s'appuie sur :

- la DNS qui correspond au secteur d'activité au titre duquel l'opérateur est désigné ;
- le PSO, dont il applique la politique de sûreté.

Le PPP doit également se conformer au plan-type défini par l'arrêté du Premier ministre du 2 juillet 2018 portant approbation du plan type de plans particuliers de protection des points d'importance vitale. Ce plan-type élaboré par le SGDSN est à la fois un guide d'aide à l'élaboration d'un PPP pour l'opérateur et un document de cadrage visant à maintenir une cohérence minimale de forme pour les plans particuliers de protection de l'ensemble des PIV situés sur le territoire national.

Par ailleurs, la législation actuelle prévoit qu'en l'absence de PSO (cas d'un opérateur qui gère ou exploite un seul PIV), le PPP doit comporter une analyse de risque.

Approbation du PPP

La décision d'approbation du PPP par le préfet de département dans le ressort duquel se trouve le PIV se fonde sur une évaluation qualitative du plan soumis par l'opérateur. Cette évaluation prend en compte :

- l'avis de la Commission zonale de défense et de sécurité (CZDS) s'il a été sollicité ;
- la conformité du plan particulier de protection par rapport au plan-type ;
- la cohérence du dispositif proposé au regard de la politique générale de protection définie par le PSO ;
- la prise en compte des prescriptions de la DNS qui s'appliquent au PIV, notamment les scénarios de menace et les objectifs de sécurité ;
- l'adéquation du dispositif proposé aux infrastructures et aux modalités d'exploitation du PIV.

En cas d'impossibilité manifeste de remplir certaines rubriques l'opérateur peut s'affranchir du plan-type dans les limites fixées par le préfet de département qui, *in fine*, approuve le PPP soumis par l'opérateur. Dans le cadre de l'approbation d'un PPP, le préfet de département sollicite l'avis d'au moins un représentant des services de police, de gendarmerie, d'incendie et de secours ou du ministère de la défense et, idéalement, l'expertise d'une administration déconcentrée ayant une compétence particulière sur le point. Il peut également effectuer une visite sur site de manière à apprécier la bonne adéquation du contenu du PPP, en vue de son approbation, avec les caractéristiques du PIV. L'approbation des PPP des PIV du secteur

nucléaire civil nécessite obligatoirement l'avis de l'autorité en charge de l'application des articles L. 1333 et suivants de l'actuel code de la défense. Un guide d'aide à l'examen du PPP a été élaboré par le ministère de l'intérieur.

A ce stade, le taux de réalisation, puis de validation des PPP peut encore être renforcé.

Mise en œuvre du PPP

Le PPP entre en vigueur le lendemain de la date de notification de la décision d'approbation. Il est décliné, en tant que de besoin, en consignes et en fiches réflexes qui ne sont pas nécessairement classifiées. Il est mis en œuvre par une organisation de sécurité définie par l'opérateur et adaptée à la nature et aux caractéristiques du point et comprenant le délégué pour la défense et la sécurité du PIV. La politique d'exercices et d'audits concourt à son évaluation, en vue de son adaptation et de son amélioration.

Révision du PPP

Le PPP peut être révisé :

- à la suite d'un contrôle portant sur la mise en œuvre du plan ;
- en cas de révision de la DNS du ou des secteurs d'activités concernés ;
- en cas de révision du PSO ;
- en cas de modification des conditions d'exploitation du PIV ou de certaines données d'environnement (urbanisation, augmentation de la délinquance, incidents de sûreté, etc.) ;
- en cas de cession du PIV ;
- à l'initiative de l'OIV.

Cette révision se fait à l'initiative de l'OIV ou sur injonction du ministre coordonnateur ou du préfet de département. Pendant toute la durée du processus de révision, le plan en vigueur continue à s'appliquer. Le plan révisé remplace le plan préexistant dès réception de l'arrêté d'approbation. Dans l'éventualité où l'opérateur contesterait le refus d'approbation du plan révisé, le PPP initial resterait en vigueur jusqu'à résolution du différend.

Modification du PPP par le préfet de département

Le préfet de département peut compléter ou modifier un PPP si l'opérateur n'a pas donné suite à l'injonction qui lui a été adressée ou si malgré les ajouts ou modifications apportés, les motifs énoncés au I de l'article R. 1332-26 de l'actuel code de la défense demeurent. Dans ce cas, le préfet de département sollicite l'avis de la CZDS sur les ajouts et modifications qu'il souhaite apporter au PPP. Ces ajouts et modifications portent sur les mesures ayant fait l'objet de l'injonction adressée à l'opérateur de compléter ou modifier ledit plan.

Diffusion du PPP

L'OIV établit, pour ce qui le concerne, les règles de diffusion interne du PPP de chacun de ses PIV, dans le respect de la réglementation relative à la protection du secret de la défense nationale. Le préfet de département, ou l'autorité militaire désignée pour le secteur « Activités militaires de l'Etat », ayant approuvé le PPP en conserve une copie, qu'il transmet également au ministre coordonnateur de l'OIV. La CIDS ou la CZDS concernée peuvent demander au préfet de département communication du PPP d'un PIV notamment en préparation d'un contrôle.

Mise en œuvre d'équivalences

Dans le domaine du transport maritime, le code des ports maritimes édicte une équivalence automatique entre les PPP et les plans de sûreté portuaire et plans de sûreté des installations portuaires approuvés (cf. articles R. 321-19 et R. 321-26 du code des ports maritimes).

Dans les autres secteurs (cf. article R. 1332-34 du code de la défense) et afin d'éviter des redondances, il appartient au préfet de département, après avis de la CIDS, de prononcer l'équivalence totale ou partielle des plans pris au titre d'autres réglementations et couvrant le domaine de la sûreté avec le PPP. Cela peut concerner, notamment, les dispositifs ci-après :

- les programmes de sûreté d'exploitant d'aéroport (PSEA) (article R. 213-1-1 du code de l'aviation civile) ;
- le plan interne de crise défini par la loi n° 2004-811 du 13 août 2004 de modernisation de la sécurité civile ;
- les plans de sûreté élaborés en application d'accords internationaux.

Le PPP de zone d'importance vitale

Une zone d'importance vitale est une aire dans laquelle sont implantés plusieurs PIV relevant d'OIV différents, pour lesquels une prise en compte commune de la sécurité présente une plus-value. Le délégué pour la défense et la sécurité de la zone d'importance vitale élabore un PPP de la zone qui prévoit des mesures communes de protection dont l'application doit être cohérente avec les mesures de protection des PIV qui constituent la zone. L'élaboration de ce plan s'appuie sur le plan-type de PPP de PIV. Les plans de sécurité des opérateurs constituant la zone d'importance vitale et leurs analyses de risque n'y sont pas annexés. Le préfet de département ou le préfet coordonnateur prend en compte le PPP de la zone d'importance vitale dans l'élaboration ou la mise à jour du plan de protection externe des PIV.

Le délégué pour la défense et la sécurité de la zone d'importance vitale, ou à défaut les OIV de la zone concernée, disposent d'un délai maximal de deux ans à partir de la date la plus récente de notification d'une DNS à l'un des opérateurs pour présenter le PPP de la zone au préfet de département ou au préfet coordonnateur. Le préfet de département ou le préfet coordonnateur dispose d'un délai de six mois à compter de la réception du PPP de la zone d'importance vitale pour statuer.

Mise en demeure et sanctions

La législation actuelle prévoit également des mesures de mise en demeure dans le cas où les opérateurs refusent de préparer leur PPP (L. 1332-4 du code de la défense). La mise en demeure des chefs d'établissement par l'autorité administrative fixe le délai pour établir le plan dans un délai qui ne peut être inférieur à un mois (L. 1332-6 du code de la défense).

Par ailleurs, des dispositions pénales sont également prévues dans le code de la défense (L. 1332-7) : « Est puni d'une amende de 150 000 euros le fait, pour les dirigeants des opérateurs mentionnés à l'article L. 1332-4 et à l'expiration du délai défini par l'arrêté de mise en demeure, d'omettre d'établir un plan de protection ou de réaliser les travaux prévus. »

Les dispositions pénales ne sont en l'espèce pas appliquées dans le dispositif actuel, ce dernier reposant sur une coopération des opérateurs, dans la mesure où l'ensemble des mesures sont prises à leurs frais.

1.1.2. Plan de protection externe (PPE)

Le plan de protection externe est un document classifié, complémentaire du PPP, réalisé par la préfecture du département dans le ressort duquel se trouve le PIV.

Dans le dispositif actuel de sécurité des activités d'importance vitale, l'actuel article R. 1332-32 du code de la défense précise les dispositions applicables concernant le plan de protection externe (PPE).

Le PPE définit les modalités d'intervention des forces de sécurité en cas d'agression sur le PIV. Il décrit et planifie les moyens humains et matériels à mettre en œuvre. A ce titre :

- sa rédaction doit associer les principaux acteurs concernés (groupement de gendarmerie départemental ou direction départementale de la sécurité publique) ;
- il doit tenir compte des éléments du PPP sans pour autant lui être redondant ;
- il doit être testé et complété en tant que de besoin ;
- il doit, dans la mesure du possible, faire l'objet d'une déclinaison par fiche d'intervention, fiches réflexes ou dossiers d'objectifs.

Il peut également prévoir des mesures de contrôle des zones périphériques au PIV et formalise les modalités d'échange d'informations avec l'opérateur (délégué pour la défense et la sécurité du PIV).

Le PPE doit également se conformer au plan-type défini par l'arrêté du Premier ministre du 2 juillet 2018 portant approbation du plan type de plans de protection externe des points d'importance vitale. Le plan-type du PPE est un document élaboré par le SGDSN. C'est à la fois un guide d'aide à l'élaboration d'un PPE pour la préfecture de département et visant à

maintenir une cohérence minimale de forme entre l'ensemble des plans de protection externe de l'ensemble des PIV situés sur le territoire national.

En cas d'actualisation du PPP d'un PIV, le préfet de département apprécie la nécessité de réviser le PPE. L'approbation d'un PPP d'une zone d'importance vitale peut entraîner la révision des PPE des PIV qui constituent cette zone, vers un PPE unique s'appliquant à ladite ZIV.

Dans le cadre de l'élaboration du PPE, le préfet de département peut être amener à effectuer une visite sur site du PIV concerné. Le préfet de département peut permettre à l'opérateur qui en fait la demande de prendre connaissance du PPE de son PIV. Il est également recommandé de communiquer le PPE aux services de police et/ou de gendarmerie compétents – dans le respect des dispositions de protection du secret de la défense nationale – dans la mesure où il leur revient d'appliquer les mesures d'intervention prévues dans ce document.

Le taux de réalisation des PPE peut encore être amélioré, notamment *via* un effort de formation des équipes préfectorales.

1.1.3. Plan de continuité d'activité

Les opérateurs d'importance vitale sont aujourd'hui tenus de réaliser, au titre des articles L. 2151-1 et L. 2151-4 du code de la défense, des plans de continuité ou de rétablissement d'activité. Ces plans ne sont aujourd'hui pas contrôlés, sur leur contenu, par l'autorité administrative, mais l'opérateur doit justifier leur élaboration. Cette planification doit permettre à l'opérateur d'identifier les personnes qui peuvent être soumises aux obligations du service de sécurité nationale définies entre les articles L. 2151-1 et L. 2151-5 du code de la défense, c'est-à-dire les individus, qui du fait de leur fonction essentielle dans l'organisation de l'opérateur désigné, peuvent être tenus de « se [maintenir] dans leur emploi habituel ou […] de le rejoindre ». Cela ne peut avoir lieu que si le conseil des ministres décide par décret de recourir au service de sécurité nationale (article L. 2151-2).

1.2. CADRE CONSTITUTIONNEL

Ce cadre reste identique à ceux précédemment décrits, c'est-à-dire le respect d'une exigence constitutionnelle de transposition des directives européennes et d'atteinte justifiée et proportionnée à la liberté d'entreprendre compte tenu des sujétions imposées aux opérateurs.

Aux termes de l'article 88-1 de la Constitution : « La République participe aux Communautés européennes et à l'Union européenne, constituées d'Etats qui ont choisi librement, en vertu des traités qui les ont instituées, d'exercer en commun certaines de leurs compétences ». Le

Conseil constitutionnel déduit de cette disposition que : « la transposition en droit interne d'une directive communautaire résulte d'une exigence constitutionnelle »[38]. Il en va de même pour une loi ayant pour objet d'adapter le droit interne à un règlement de l'Union européenne[39].

Les obligations de réaliser les plans (PPE, PPE, plan de continuité) à la charge des OIV, dont le manquement pouvant être sanctionné au niveau administratif, porte nécessairement une atteinte à la liberté d'entreprendre, laquelle découle de l'article 4 de la Déclaration des droits de l'Homme et du Citoyen de 1789[40]. Cette atteinte ne peut être ni générale ni absolue[41]. Le législateur peut limiter l'exercice de cette liberté à la condition qu'il n'en résulte pas d'atteintes disproportionnées au regard de l'objectif poursuivi[42], alors même que cette atteinte résulterait de l'exigence constitutionnelle de transposition adéquate des directives européennes[43], dans un objectif de sécurité et de défense de la Nation, en l'absence de disposition spécifique contraire de la Constitution[44] ou de mise en cause d'une règle ou d'un principe inhérent à notre identité constitutionnelle[45].

Enfin, en l'absence de remise en cause de ses garanties fondamentales, la liberté du commerce et de l'industrie ne s'oppose pas à l'intervention du législateur dans ce domaine[46].

1.3. CADRE CONVENTIONNEL

Au niveau européen, la directive (UE) 2022/2557 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience des entités critiques (REC) permet désormais d'offrir un socle minimal commun de résilience à tous les opérateurs de l'UE. Elle doit être transposée dans notre droit national d'ici le 17 octobre 2024.

Son champ d'application couvre 11 secteurs : énergie, transports, infrastructures bancaires, infrastructures de marché financier, santé, eau potable, assainissement, infrastructures digitales, administration publique (niveau central), espace, alimentation.

---

[38] Voir notamment la décision n° 2004-496 DC du 10 juin 2004, « Loi pour la confiance dans l'économie numérique ».

[39] Voir par exemple la décision n° 2018-765, « Loi relative à la protection des données personnelles », considérant 3.

[40] Conseil constitutionnel, décision 98-401 DC du 10 juin 1998.

[41] Décision 82-141 DC du 27 juillet 1982.

[42] Décision 2023-1055 QPC du 16 juin 2023.

[43] Décision 2006-535 DC du 30 mars 2006.

[44] Décision 2004-497 DC du 1er juillet 2004.

[45] Décision 2018-765 DC du 12 juin 2018 ; décision 2019-818 QPC du 6 décembre 2019.

[46] Décision 2003-474 DC du 17 juillet 2003.

La directive REC consacre le passage d'une logique de protection d'infrastructures critiques physiques à une logique de résilience des entités critiques (article 1er), qui met davantage l'accent sur la continuité de leur activité, en sus de la protection physique de leurs installations.

L'article 13 de la directive prévoit que :

« Les États membres veillent à ce que les entités critiques aient mis en place et appliquent un plan de résilience ou un ou plusieurs documents équivalents, qui décrivent les mesures prises (…). Lorsque les entités critiques ont élaboré des documents ou pris des mesures en vertu d'obligations prévues dans d'autres actes juridiques qui sont (…), elles peuvent utiliser ces documents et mesures pour satisfaire aux exigences énoncées dans le présent article. Dans l'exercice de ses fonctions de supervision, l'autorité compétente peut déclarer que des mesures existantes de renforcement de la résilience prises par une entité critique qui portent, de manière appropriée et proportionnée, sur les mesures techniques, les mesures de sécurité et les mesures organisationnelles (…) respectent, en tout ou en partie, les obligations prévues par le présent article. »

1.4. ELEMENTS DE DROIT COMPARE

Sans objet**.**

2. NECESSITE DE LEGIFERER ET OBJECTIFS POURSUIVIS

2.1. NECESSITE DE LEGIFERER

La directive européenne sur la résilience des entités critiques (REC) du 14 décembre 2022 consacre le passage d'une logique de protection d'infrastructures critiques physiques à une logique de résilience des entités critiques. Les opérateurs ne sont plus seulement tenus de protéger leurs installations et matériels. Ils sont tenus de s'assurer de la résilience de l'activité pour laquelle ils ont été désignés.

Dans le cadre de la transposition, il apparaît opportun de prendre en compte au niveau législatif la notion de « plan de résilience », qui figure expressément dans la directive, et qui n'existe pas dans le dispositif actuel.

Tout changement dans l'actuel Plan de sécurité opérateur (PSO) entraine la mise à jour des plans de protection des sites (PPP et PPE). Dans la mesure où le nouveau dispositif prévoit la création d'un plan de résilience opérateur (PRO) en lieu et place du PSO, il convient ainsi de modifier les plans de protection au niveau des PIV.

Par ailleurs, l'article 34 de la Constitution impose de recourir à la loi, pour les mêmes motifs que ceux précédemment rappelés s'agissant d'une mesure d'organisation de la défense nationale laquelle impose des sujétions à des opérateurs qui peuvent être des collectivités territoriales ou des opérateurs privés intervenant dans un secteur concurrentiel.

2.2. OBJECTIFS POURSUIVIS

Le premier objectif poursuivi est la conservation des grands principes du dispositif actuel tout en incluant une dimension « résilience » à la planification de la protection des sites.

3. OPTIONS ENVISAGEES ET DISPOSITIF RETENU

3.1. OPTIONS ENVISAGEES

Il a été envisagé de conserver le dispositif actuel avec les PPP et PPE en ajoutant un plan de résilience à réaliser pour les PIV. Cependant, il est apparu qu'une telle option alourdirait le processus actuel et serait de nature à créer de la confusion chez les opérateurs et les préfectures.

3.2. DISPOSITIF RETENU

La présente mesure consacre la création du « Plan particulier de résilience » (PPR) qui remplace l'actuel Plan particulier de protection (PPP) propre à chaque PIV. Il a également pour vocation d'intégrer les éléments auparavant indiqués dans le PPE en annexe, ainsi qu'une partie des éléments qui pouvaient apparaitre auparavant dans le plan de continuité d'activité que l'opérateur devait effectuer au titre de l'article L. 2151-4.

Ainsi l'impératif de résilience est pris en compte sans lourdeur supplémentaire pour les opérateurs ou les préfectures, et la complémentarité entre l'Etat et l'opérateur qui est l'un des principes majeurs du dispositif de sécurité des activités d'importance vitale se matérialise dans un document unique. Le choix de ce dispositif vise également à assurer une cohérence avec le plan de résilience opérateur (PRO) décrit *supra*.

On remarquera que le présent article aligne les mesures de police administrative qui viennent compléter le dispositif actuel sur les mesures prévues supra pour les PRO, l'impératif de clarté et de simplification étant au cœur de la réflexion.

4. ANALYSE DES IMPACTS DES DISPOSITIONS ENVISAGEES

4.1. IMPACTS JURIDIQUES

4.1.1. Impact sur l'ordre juridique interne

La présente mesure remplace l'article L. 1332-5 du code de la défense et introduit dans le droit national la notion de plan particulier de résilience (PPR). Dans un second temps, il est prévu que soit ajouté le PPE en annexe de ce nouveau plan particulier de résilience afin de simplifier le processus de planification au niveau des PIV et son approbation. La trame indicative sera proposée dans les actes réglementaires.

L'article L. 2151-4 est modifié par l'article 2 du présent projet de loi pour tenir compte de cette évolution.

Ces dispositions portent une atteinte à la liberté d'entreprendre et à la liberté du commerce et de l'industrie qui est proportionnée et en rapport avec l'objectif poursuivi se rattachant à la défense et à la sécurité nationale.

Par ailleurs, le remplacement des dispositions des actuels articles L. 1332-1 et L. 1332-2 du code de la défense implique d'en tirer les conséquences dans les dispositions de droit interne qui font référence, selon les cas, à certains établissements, installations ou ouvrages, relevant de l'article L. 1332-1 (actuel), lesquels correspondront aux infrastructures critiques des opérateurs d'importance vitale.

Cet impact ne se limite pas aux seuls établissements, installations, ouvrages mais peut également concerner les opérateurs eux-mêmes, lesquels seront désormais qualifiés par la loi d'opérateurs d'importance vitale qui seront distincts selon les modalités de désignation, au titre du 1° ou du 2° du I de l'article L. 1332-2.

Enfin, les modifications prévues s'agissant des documents de planification ont entraîné des impacts sur les dispositions internes y faisant référence.

Toutes ces modifications induites ont été regroupées au sein d'un article 2, qui procède intégralement aux modifications nécessaires. Ces dispositions n'ont par elles-mêmes aucun autre impact que celui de modifier des références textuelles.

4.1.2. Articulation avec le droit international et le droit de l'Union européenne

Les dispositions de la présente mesure s'inscrivent dans le champ de la transposition de la directive européenne sur la résilience des entités critiques du (REC) du 14 décembre 2022, notamment son article 13.

Le troisième alinéa des dispositions prévues dans le présent article précise les cas où une équivalence au PPR est possible. L'objectif est de prendre en compte des normes

internationales déjà existantes, notamment dans le domaine maritime et portuaire où des opérateurs déjà soumis au code ISPS (*International Ship and Port Facility Security*) ne sont pas tenus de réaliser de PPP quand leurs plans de sûreté sont conformes au code et validés par les instances concernées.

4.2. IMPACTS ECONOMIQUES ET FINANCIERS

4.2.1. Impacts macroéconomiques

Les mesures de résilience prévues pourront engendrer des coûts supplémentaires pour un opérateur. Si la logique de protection physique était déjà prise en compte, la systématisation de la prise en compte de la continuité d'activité ne sera en effet pas neutre. Ces coûts sont extrêmement difficiles à évaluer tant les opérateurs de la SAIV opèrent dans des secteurs diversifiés et à différentes échelles.

Néanmoins, le principe de résilience – au cœur de cette transposition – permettra *in fine* à l'opérateur et – au regard de certaines dépendances – à l'ensemble du tissu économique de pouvoir maintenir son activité dans un contexte dégradé et vise à amortir les coûts imputables à la disruption de son activité.

4.2.2. Impacts sur les entreprises

Les mesures de résilience prévues dans les présentes dispositions peuvent engendrer des coûts supplémentaires pour un opérateur privé. Si la logique de protection physique était déjà prise en compte par les opérateurs, la systématisation de la prise en compte de la continuité d'activité ne sera pas neutre. Ces coûts sont extrêmement difficiles à évaluer tant les opérateurs de la SAIV opèrent dans des secteurs diversifiés et à différentes échelles.

Néanmoins, la mise en œuvre de mesures de résilience permet à l'opérateur de maintenir son activité dans un contexte dégradé, contribuant à prévenir des coûts potentiellement bien supérieurs en cas de disruption de son activité. En outre, la résilience accrue de l'ensemble des opérateurs est de nature également à prévenir l'apparition de coûts en cas de disruption de l'activité d'un fournisseur pour les mêmes motifs.

4.2.3. Impacts budgétaires

Le nouveau dispositif n'entraine pas de changement quant au mode de coopération avec les OIV publics et privés, qui continueront de contribuer à leurs frais.

La transformation du PPP en PPR ainsi que l'addition du PPE en annexe de ce dernier impliquera des coûts supplémentaires limités, qu'il convient de mettre en perspective avec les coûts majeurs d'une interruption totale de leurs activités.

4.3. IMPACTS SUR LES COLLECTIVITES TERRITORIALES

Les dispositions de la présente mesure n'entraînent pas d'impact supplémentaire pour les collectivités territoriales par rapport au dispositif actuellement en vigueur. Certaines collectivités territoriales sont en effet déjà désignées opérateur d'importance vitale en raison des activités qu'elles assurent pour leurs administrés. Le changement d'appellation de PPR (à la place de PPP) n'aura ainsi qu'un impact marginal.

4.4. IMPACTS SUR LES SERVICES ADMINISTRATIFS

La simplification du processus d'élaboration et de validation de PPR aura pour effet une simplification du dispositif sur les services administratifs. Cela aura toutefois pour conséquence d'obliger les services administratifs – délégation militaire départementale pour les PIV militaires comme préfectures pour les PIV civils – de vérifier la bonne prise en compte et mise en place de mesures de continuité d'activité par les opérateurs, ce qui n'était autrefois pas vérifié.

De plus, la directive européenne induit la nécessité d'études périodiques de l'évaluation des risques.

De l'analyse des risques découle la rédaction du PRO puis du PPR, impliquant que ces derniers devront être revus au moins tous les quatre ans, faisant peser une charge supplémentaire sur les services administratifs concourants à toute la chaîne d'élaboration des plans mentionnée *supra* : préfectures, zones de défense et de sécurité, SGDSN. Un besoin en ressources humaines supplémentaires peut ici être envisagé.

4.5. IMPACTS SOCIAUX

4.5.1. Impacts sur la société

Le renforcement des exigences en matière de résilience des activités d'importance vitale doit permettre de limiter les impacts d'une crise ou de problèmes majeurs d'un opérateur d'importance vitale sur le fonctionnement de la société.

4.5.2. Impact sur les personnes en situation en handicap

Sans objet.

4.5.3. Impacts sur l'égalité entre les femmes et les hommes

Sans objet.

4.5.4. Impacts sur la jeunesse

Sans objet.

4.5.5. Impacts sur les professions réglementées

Sans objet.

4.6. IMPACTS SUR LES PARTICULIERS

Sans objet.

4.7. IMPACTS ENVIRONNEMENTAUX

Sur cet enjeu, la disposition prévue n'apporte pas de modification quant au dispositif actuel.

5. CONSULTATIONS MENEES ET MODALITES D'APPLICATION

5.1. CONSULTATIONS MENEES

Une concertation de l'ensemble des ministères coordonnateurs a été réalisée sur cette mesure.

En application de l'article L. 1212-2 du code général des collectivités territoriales, le présent article a été soumis à l'examen du Conseil national d'évaluation des normes qui a rendu un avis défavorable le 22 mai 2024.

Enfin, le service national des enquêtes administratives de sécurité, le coordinateur général de la sécurité nucléaire, le service juridique du Secrétariat général des affaires européennes et l'Agence nationale de sécurité des systèmes d'informations ont également été consultés.

5.2. MODALITES D'APPLICATION

5.2.1. Application dans le temps

Les présentes dispositions entrent en vigueur le lendemain de la publication de la présente loi au *Journal officiel* de la République française.

Les opérateurs d'importance vitale désignés avant l'entrée en vigueur des dispositions du titre I^{er} de la présente loi doivent être regardés comme désignés en application du I de l'article

L. 1332-2 du code de la défense dans sa rédaction résultant du chapitre I[er] de la loi à la date de son entrée en vigueur.

Ces opérateurs restent soumis aux obligations qui leurs sont applicables avant l'entrée en vigueur de la présente loi jusqu'à l'accomplissement des obligations prévues aux articles L. 1332-2 à L. 1332-5 et à l'article L. 1332-11 dans leur rédaction résultant de la présente loi.

5.2.2. Application dans l'espace

Le présent article est applicable de plein droit sur l'ensemble du territoire de la République conformément à l'article L. 1 du code de la défense.

Aussi, les dispositions du code de la défense créées par le présent projet de loi seront applicables de plein droit à la fois dans les collectivités régies par le principe de l'identité législative (la Guadeloupe, la Guyane, la Martinique, La Réunion, Mayotte, Saint-Barthélemy, Saint-Martin et Saint-Pierre-et-Miquelon) et par le principe de la spécialité législative (les îles Wallis et Futuna, la Polynésie française, la Nouvelle-Calédonie et les Terres australes et antarctiques françaises).

En tant que PTOM, le droit de l'union européenne ne s'applique pas à Saint-Barthélemy, Saint-Pierre-et-Miquelon, dans les îles Wallis et Futuna, en Polynésie française, Nouvelle-Calédonie et dans les Terres australes et antarctiques françaises. Les dispositions applicables aux seuls OIV exerçant des services essentiels au fonctionnement du marché intérieur de l'Union européenne ne seront donc pas applicables en l'absence d'adaptation.

5.2.3. Textes d'application

Le présent article fera l'objet d'un décret en Conseil d'Etat afin de préciser les modalités d'élaboration des plans particuliers de résilience.

Article 1er (F) – Article L. 1332-6 du code de la défense – Enquêtes administratives de sécurité

1. ETAT DES LIEUX

1.1. CADRE GENERAL

Une introduction des enquêtes administratives de sécurité dans la loi LOPPSI 2.

Le dispositif de contrôle de l'accès aux points d'importance vitale, qui permet aux opérateurs désignés OIV de demander la réalisation d'enquêtes administratives de sécurité, a été créé par la loi n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure (dite loi « LOPPSI 2 »). Les dispositions d'application ont été fixées par le décret n° 2012-491 du 16 avril 2012.

L'argumentaire mis en avant dans le rapport soumis à l'Assemblée Nationale et permettant de justifier l'instauration de cette mesure était que, si les opérateurs privés comme publics devaient coopérer à leur frais afin d'assurer la protection de leurs sites les plus sensibles, certaines dispositions relatives à l'accès des sites devaient être ajoutées. Le rapport[47] indique en effet que le dispositif n'était « *pas complet dans la mesure où il ne comporte pas de dispositions relatives à l'accès à ces installations d'importance vitale* ».

La mise en œuvre de cette disposition permettait de plus d'harmoniser les pratiques : en effet, certains sites disposaient déjà de la possibilité de réaliser des procédures d'accès réglementé contrôlées par le préfet.

L'introduction de cet article dans la LOPPSI 2 avait donc pour but de donner à l'opérateur la possibilité de demander une enquête administrative de sécurité pour toutes les installations identifiées comme d'importance vitale, en se fondant sur deux principes :

- Dans tous les cas, l'accès à tout ou partie de ces zones peut être réglementé par le gestionnaire de l'établissement, installation ou ouvrage ;
- La décision d'autorisation d'accès pourra être précédée d'une demande d'avis à l'autorité administrative, dans des conditions et selon les modalités précisées par décret en Conseil d'Etat. Un opérateur d'importance vitale ne devait donc pas avoir à systématiquement demander une enquête administrative pour autoriser l'accès à l'ensemble de ses installations.

[47] N° 2271 - Rapport de M. Éric Ciotti sur le projet de loi d'orientation et de programmation pour la performance de la sécurité intérieure (n°1697) (assemblee-nationale.fr).

Le rapport en question établissait en effet que les besoins relatifs au contrôle d'accès pour chaque secteur d'activité devaient être identifiés dans les directives nationales de sécurité.

Après la parution du décret d'application n° 2012-491 du 16 avril 2012, les opérateurs d'importance vitale ont donc obtenu la possibilité de demander la réalisation d'une enquête administrative de sécurité. Cette enquête, devant être réalisée en une dizaine de jours, permet la consultation de différents types de fichiers :

- les fichiers d'antécédents judiciaires ;
- les fichiers de personnes recherchées ;
- les fichiers de services chargés de l'information générale (traitement de données relatif à la prévention des atteintes à la sécurité publique) ;
- les fichiers de renseignement.

Ces fichiers consultables sont régis par l'article 26 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. Dans le cadre de la procédure, les services enquêteurs peuvent également avoir accès au bulletin n°2 du casier judiciaire. Ils ne peuvent par contre avoir accès aux fichiers d'identification. La disposition existante précise également que la personne demandant l'accès au site ait connaissance de la procédure en cours.

Procédure de la demande d'avis à l'autorité administrative

La saisine pour avis du préfet ou de l'autorité militaire compétente, en ce qu'elle permet la réalisation d'une enquête administrative sur des personnes accédant à un PIV, participe au dispositif général de prévention de ces sites contre tout acte de malveillance. La procédure répond aujourd'hui au principe de complémentarité du dispositif entre l'Etat et l'opérateur. Elle contribue, en amont, à la protection des composants les plus névralgiques d'un point d'importance vitale. Si la décision d'autorisation d'accès d'une personne à un point d'importance vitale relève bien du seul opérateur, l'administration lui apporte son concours dans ce processus décisionnel. Les articles R. 1332-22-1 à R. 1332-22-3 précisent l'actuel article L. 1332-2-1 du code de la défense en prévoyant la procédure par laquelle, avant d'autoriser l'accès d'une personne à un point d'importance vitale qu'il gère, l'opérateur peut solliciter l'avis du préfet de département dans lequel est situé le PIV.

Pour les opérateurs d'importance vitale dont le ministre coordonnateur est le ministre de la défense, leur demande d'avis est adressée à l'autorité militaire désignée (service enquêteur du ministère de la défense).

Pour les opérateurs d'importance vitale relevant du domaine nucléaire, leur demande d'avis est adressée directement au commandement spécialisé pour la sécurité nucléaire (CoSSeN) depuis la création du service en question le 20 avril 2017. Le CoSSeN, service à compétence

nationale rattaché à la direction générale de la gendarmerie nationale, dispose d'un département chargé d'« *assurer le contrôle et le suivi administratif des personnes accédant aux installations nucléaires ainsi que la maitrise des risques métier inhérents à la sécurité des activités nucléaires. Le département comprend le bureau des accédants du nucléaire chargé d'assurer le suivi et le contrôle de toutes les personnes physiques et morales qui sont amenées à accéder aux installations concourant aux activités nucléaires ou à des informations classifiées à ce titre* » (article 3 de l'arrêté du 20 avril 2017 portant organisation et fonctionnement du service à compétence nationale dénommé « Commandement spécialisé pour la sécurité nucléaire »).

De manière à faciliter les échanges et à réduire les temps de traitement de l'enquête par les services territoriaux compétents, la demande doit, dans la mesure du possible, être émise par le délégué à la défense et à la sécurité (DDS) du PIV concerné. La demande d'avis doit être signée par le DDS et adressée par écrit dématérialisé au préfet du département (préfet de police, le cas échéant), à l'autorité militaire dans lequel se situe le PIV ou sur la plateforme dédiée à cette demande du CoSSeN.

Elle doit impérativement comporter les informations suivantes, regroupées en trois rubriques :

Données relatives à l'opérateur et au PIV :

- année / numéro d'ordre de la demande pour le PIV concerné ;
- numéro de triplet.

Données relatives à la personne :

- nom et prénom(s) ;
- date et lieu de naissance ;
- domicile actuel ;
- nom de l'employeur (si différent du demandeur) ;
- profession.

Données relatives à l'accès au site :

- désignation, conformément au zonage codifié dans le PPP, de la partie ou des parties du PIV justifiant une demande d'avis en vue de l'accès ;
- justification de la nécessité de l'accès à la partie du PIV concernée ;
- justification de l'impossibilité de mettre en place des mesures de prévention autres ;
- durée prévue de l'accès au site (date, durée, période et répétition éventuelle) ;
- numéro d'immatriculation du véhicule (si l'accès en véhicule est sollicité).

Aucun élément d'identification du PIV ou de l'opérateur (charte graphique, logo, etc.) ne doit figurer sur le document transmis de manière à ce qu'il puisse être acheminé par voie

dématérialisée. Il revient à l'opérateur, dans son intérêt propre, d'effectuer la demande le plus en amont possible de la date prévue d'accès au point d'importance vitale. Dans la mesure du possible, et sauf exception précisée infra, l'opérateur sollicite les services préfectoraux au minimum 3 semaines avant la venue effective sur site de la personne concernée.

De la même manière, et sauf exception, l'OIV dont le ministre coordonnateur est le ministère chargé de la défense sollicite l'autorité militaire désignée au minimum 2 mois avant la venue effective sur site de la personne concernée.

En cas d'urgence dûment justifiée par l'OIV, ce délai de sollicitation peut être réduit à 72 h. Les services préfectoraux instruisent alors la demande en priorité afin, dans la mesure du possible, de rendre un avis dans les délais compatibles avec la date prévue de l'accès au PIV par la personne concernée. Cette procédure exceptionnelle ne doit aucunement venir palier un défaut d'organisation interne de l'opérateur. Le recours à cette procédure ne peut en aucun cas revêtir un caractère systématique. La demande devra être transmise à la préfecture ou à l'autorité militaire selon la procédure dématérialisée habituelle en utilisant le document prévu pour celle-ci. Dans tous les cas, la production de l'avis par l'administration n'est pas un préalable obligatoire à l'accès d'une personne à un point d'importance vitale.

Encadrement des possibilités de demandes d'avis

Conformément aux dispositions légales et réglementaires, les demandes d'avis adressées à l'administration sont encadrées au regard, d'une part, des lieux compris dans le PIV auquel il est accédé (encadrement *ratione loci*) et, d'autre part, des personnes accédant à ces lieux (encadrement *ratione personae*) :

- Encadrement *ratione loci* de la demande d'avis

La demande d'avis ne peut concerner que l'accès aux parties du PIV devant faire l'objet d'une surveillance particulière car présentant une vulnérabilité spécifique au regard des scénarios de menaces retenues. Ces parties du PIV doivent être précisément identifiées dans le PPP (zonage codé). Elles peuvent correspondre, en tout ou en partie, aux composants névralgiques identifiés par le PPP. Les zones dont l'accès sera soumis au dispositif SAIV doivent être explicitement mentionnées dans le PPP en référençant notamment l'article R. 1332-22-1 du code de la défense. Il faut exclure, par exemple, les zones recevant temporairement ou de façon permanente du public telles que les postes d'accueil, les salles de réunion ou les salles de conférence. De même, les PIV sans dispositif de filtrage et de contrôle des accès sont exclus du dispositif.

- Encadrement *ratione personae* de la demande d'avis

Conformément à l'article R. 1332-22-2 de l'actuel code de la défense, deux catégories de personnes ne peuvent faire l'objet d'une demande d'avis quant à leur accès aux PIV :

- les personnes mentionnées par le décret n° 2005-1124 du 6 septembre 2005 fixant la liste des enquêtes administratives donnant lieu à la consultation des traitements automatisés de données personnelles mentionnés à l'article 230-6 du code de procédure pénale. En effet, du fait de leur emploi ou des fonctions qu'elles occupent lors de leur accès au PIV, ces personnes ont déjà fait l'objet d'une enquête administrative.
- les personnes dont l'accès au PIV fait l'objet de mesures de prévention et de sécurité suffisantes.

Il s'agit là des personnes qui, du fait notamment de la nature et de la durée de leur accès au site, peuvent faire l'objet d'un contrôle suffisant rendant inutile la réalisation d'une enquête administrative, et donc la formulation d'une demande d'avis auprès de l'administration. Il peut, par exemple, s'agir de personnes effectuant une courte visite du PIV et pouvant être accompagnées durant cette visite ou de personnes (stagiaires…) ne pouvant accéder aux parties les plus sensibles du PIV du fait de dispositifs d'accès restreint aux différentes parties du PIV.

Par ailleurs, sont exclues de l'application du dispositif l'ensemble des personnes ayant à accéder à un PIV à l'occasion d'une ouverture au public et ce quel qu'en soit la forme (conférences, journées portes ouvertes, etc.). Le PPP doit préciser les mesures de prévention et de sécurité mises en place pour contrôler l'accès aux différentes parties du PIV selon la raison pour laquelle cet accès s'effectue.

Avant de réaliser une enquête administrative, les services préfectoraux s'assurent que la demande d'avis formulée par l'OIV ne contrevient pas à ces critères *ratione loci* et *ratione personae*. Toute demande d'avis doit donc être justifiée au regard de ces critères. A défaut, elle sera rejetée par utilisation d'un formulaire de rejet dédié à cet effet.

<u>Information de la personne accédant au PIV par l'opérateur d'importance vitale</u>

L'opérateur doit obligatoirement notifier par écrit à la personne concernée qu'il a sollicité l'avis de l'administration quant à son accès au site et que, dans, ce cadre, conformément aux dispositions législatives et réglementaires en vigueur, elle fait l'objet d'une enquête administrative.

Il peut pour cela s'appuyer sur la formulation suivante :

« Dans le cadre de … (raison de l'accès au site), vous allez être amené(e) à accéder à un/des site(s) relevant de la responsabilité de notre société. Afin de sécuriser l'accès à ce(s) site(s), et conformément aux dispositions législatives et réglementaires en vigueur, nous avons sollicité préalablement l'avis de l'autorité administrative. Dans ce cadre, une enquête administrative destinée à vérifier qu'aucun fait vous concernant n'est incompatible avec l'accès envisagé est susceptible d'être réalisée par l'autorité administrative. »

Cette notification ne doit pas faire apparaitre les raisons exactes qui prévalent au déclenchement d'une enquête. En particulier, le caractère très sensible de telle ou telle partie du point d'importance vitale ne doit pas être porté à la connaissance de la personne visée par l'enquête.

Sens de l'avis et durée de validité

Si la demande de l'opérateur est jugée recevable, le préfet émet un avis sur la compatibilité des caractéristiques de la personne avec l'accès au PIV envisagé. Afin d'émettre cet avis, une enquête administrative est diligentée.

- Sens de l'avis

A la suite de l'enquête administrative, le préfet transmet à l'opérateur d'importance vitale un avis précisant si les caractéristiques de la personne concernée sont « compatibles » ou « incompatibles » avec l'accès aux zones désignées du PIV. Cet avis, qui n'est pas une décision administrative, n'est pas motivé. Il n'est pas contraignant pour l'OIV qui reste le seul responsable de l'accès d'une personne au site dont il a la charge.

- Durée de validité de l'avis

L'avis formulé par l'administration est valable pour une durée de trois ans. Ce délai doit être entendu comme le terme avant lequel l'OIV ne sollicitera pas à nouveau l'administration pour l'accès de la même personne au même PIV. Néanmoins, si les conditions nécessaires à la délivrance de l'avis évoluent, c'est-à-dire que des changements radicaux de situation ou de comportement sont notés par le délégué à la défense et à la sécurité du site concerné, l'opérateur peut solliciter un nouvel avis de l'administration qui jugera de l'opportunité de conduire à nouveau une enquête.

Principes et cadre de l'enquête administrative

Conformément aux dispositions des articles L. 1332-2-1 et R. 1332-22-1 du code de la défense, l'enquête administrative peut donner lieu à la consultation du bulletin n° 2 du casier judiciaire ainsi que des traitements automatisés de données à caractère personnel relevant de l'article 26 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. Les fichiers d'identification ne peuvent cependant pas être consultés.

Les services, civils ou militaires, en charge de l'enquête administrative doivent pouvoir s'appuyer sur l'ensemble des traitements automatisés de données visés au paragraphe précédent quel que soit l'organisme de gestion. Une collaboration efficace doit donc être mise en place entre les services du ministère de l'intérieur et ceux du ministère chargé de la défense afin de s'assurer que tous les traitements automatisés de données opportuns soient consultés, sans qu'il en résulte pour autant une obligation de communication compte tenu de la nature de certaines informations.

Ainsi, en tant que de besoin, les services du ministère de l'intérieur peuvent solliciter le concours des services du ministère chargé de la défense dans le cadre des demandes d'avis émanant d'opérateurs ne relevant pas du ministère chargé de la défense et, réciproquement, les services du ministère chargé de la défense peuvent solliciter le concours de ceux du ministère de l'intérieur pour les demandes d'avis émanant d'opérateur relevant du ministère chargé de la défense.

Le dispositif de contrôle d'accès aux points d'importance vitale ne se substitue pas aux dispositifs déjà existants fondés sur d'autres bases légales et permettant le contrôle de l'accès à des zones spécifiques.

Les enquêtes peuvent également avoir accès aux fichiers européens dédiés à cet effet – par exemple le système d'information Schengen (SIS) via le système ACCReD (automatisation de la consultation centralisée de renseignements et de données) créé en 2017, mais aussi au système européen d'information sur les casiers judiciaires (ECRIS), qui permet aux Etats européens d'échanger sur les condamnations d'un ressortissant national et devrait sous peu permettre aux Etats européens d'échanger sur les condamnations effectuées sur leur territoire pour des ressortissants étrangers (cette disposition doit être mise en œuvre en 2024).

Portée de l'avis rendu pour les opérateurs

Sur le sujet des enquêtes administratives de sécurité, le Conseil d'Etat, lors de l'examen du projet de loi relatif aux jeux Olympiques et Paralympiques de 2024 et portant diverses autres dispositions, a émis l'avis suivant :

« Le Conseil d'Etat examine ensuite l'article L. 211-11-1 au regard de l'article 12 de la Déclaration des droits de l'homme et du citoyen de 1789 dont il découle qu'une personne privée ne peut être investie de pouvoirs de police administrative générale, inhérente à l'exercice de la force publique (Décision n° 2011-625 DC du 10 mars 2011 systèmes de vidéo protection sur la voie publique).

Il constate que l'article L. 211-11-1 crée un dispositif destiné à assurer la sécurité de grands événements auquel le Gouvernement peut décider de recourir par décret en cas de risque exceptionnel de menace terroriste, qui repose sur le contrôle par l'organisateur de l'accès aux équipements et installations qui accueillent ces grands événements des personnes autres que les spectateurs et les participants.

A l'occasion des jeux Olympiques et Paralympiques de 2024, l'article L. 211-11-1 est susceptible de s'appliquer à des événements d'une ampleur exceptionnelle dans des lieux fréquentés par des millions de personnes, y compris dans des installations mises en place dans des espaces publics. Ce dispositif devrait, selon les informations transmises par le Gouvernement, conduire les organisateurs des jeux Olympiques et Paralympiques à prendre, après autant d'enquêtes administratives, près de 750 000 décisions relatives à l'accès des

personnes autres que les spectateurs aux installations et équipements dans lesquels se dérouleront ou seront retransmis les événements.

Alors que ces décisions d'autorisation d'accès constituent l'élément central de ce dispositif de sécurité, l'article L. 211-11-1 reconnait aux organisateurs un pouvoir discrétionnaire. Il laisse l'organisateur libre d'autoriser l'accès à ces lieux à des personnes qui auraient fait l'objet d'un avis défavorable de l'autorité administrative, étant rappelé que selon son deuxième alinéa « un avis défavorable ne peut être émis que s'il ressort de l'enquête administrative que le comportement ou les agissements de la personne sont de nature à porter atteinte à la sécurité des personnes, à la sécurité publique ou à la sûreté de l'Etat ». Le texte confie ainsi à l'organisateur le pouvoir de prendre une mesure de police.

Pour ces raisons le Conseil d'Etat considère que l'article L. 211-11-1 délègue à des personnes privées des compétences de police administrative générale inhérentes à l'exercice de la « force publique », cette délégation étant amplifiée par le projet, et qu'il méconnait par suite l'article 12 de la Déclaration de 1789. Aussi, afin de ne pas exposer les dispositions du projet à cette inconstitutionnalité, le Conseil d'Etat propose que la décision d'autorisation d'accès de l'organisateur soit rendue sur avis conforme de l'autorité administrative. Il modifie le projet en ce sens. »

L'assimilation du pouvoir de déroger à un avis défavorable à une mesure de police administrative, non délégable à une personne privée, exige ainsi de rendre conforme l'avis dispensé à tout opérateur d'importance vitale privé pour toute personne ayant accès à un point ou une zone sensible du point d'importance vitale.

Volume du nombre d'enquêtes effectuées

Compte tenu des différents secteurs d'activités d'importance vitale, plusieurs services enquêteurs sont chargés de réaliser les enquêtes administratives de sécurité au titre du dispositif :

- Le Service National des Enquêtes Administratives de Sécurité (SNEAS), saisi pour tous les sites des opérateurs civils par les préfectures sur demande des opérateurs. Ce service, qui réalise annuellement 700 000 enquêtes, estime à 70 000 le nombre d'enquêtes 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, saisie pour tous les sites relevant du ministère chargé de la défense. La direction estime réaliser 300 000 enquêtes pour les points d'importance vitale relevant de leurs secteurs d'activités (activités militaires de l'Etat et activités de l'industrie de l'armement) mais aussi pour les besoins d'habilitations du ministère ;

- Le Commandement spécialisé pour la sécurité nucléaire (CoSSeN), saisi pour les sites relevant du domaine nucléaire, étant donné que le secteur a des obligations spécifiques en termes de mesures de sureté. L'organisme estime réaliser environ 396 000 enquêtes annuelles, avec moins d'1 % d'avis défavorables (2569 très exactement pour l'année 2022).

Recours administratif

Si la décision finale de suivre ou non l'avis transmis par l'autorité administrative reste à la main de l'opérateur – il est rappelé que la motivation de l'avis n'est jamais transmise à ce dernier –, la personne ayant fait l'objet d'un avis négatif pour laquelle l'accès à un point d'importance vitale peut avoir été refusé a la possibilité d'effectuer un recours administratif préalable obligatoire (RAPO). Ce dernier est effectué auprès du ministère coordonnateur, en sa qualité d'autorité administrative et au vu des dispositions de l'article R. 1332-33. Le ministère coordonnateur peut donc changer, s'il l'estime nécessaire, la décision d'accès ou non au site d'importance vitale, décision qui peut être contestée devant un tribunal administratif.

1.2. CADRE CONSTITUTIONNEL

En premier lieu, le Conseil constitutionnel a déjà été conduit à déclarer conforme à la Constitution les dispositions de l'article 25 de la loi n° 2003-239 du 18 mars 2003 pour la sécurité intérieure pérennisant le principe des enquêtes administratives de sécurité et en étendant le champ d'intervention possible[48].

De telles dispositions portent nécessairement atteinte à la liberté d'entreprendre, à la liberté de circulation et au droit d'obtenir un emploi découlant de l'alinéa 5 du Préambule de la Constitution de 1946[49].

Toutefois, comme déjà rappelé, dès lors qu'elle est proportionnée et justifiée, le législateur peut y porter une atteinte strictement limitée aux objectifs d'ordre public et de défense nationale poursuivis. Et cette atteinte, dès lors qu'elle se concilie, sans erreur manifeste, avec le droit de chacun d'obtenir un emploi, comme c'est le cas en l'espèce, le législateur ne méconnaît pas la Constitution[50].

1.3. CADRE CONVENTIONNEL

[48] Décision 2003-467 DC du 13 mars 2003.

[49] Décision 2012-654 DC du 9 août 2012.

[50] Décision 2004-509 DC du 13 janvier 2005.

Au niveau européen, la directive (UE) 2022/2557 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience des entités critiques (REC) permet désormais d'offrir un socle minimal commun de résilience à tous les opérateurs de l'UE. Elle doit être transposée dans notre droit national d'ici le 17 octobre 2024.

Son champ d'application couvre 11 secteurs : énergie, transports, infrastructures bancaires, infrastructures de marché financier, santé, eau potable, assainissement, infrastructures digitales, administration publique (niveau central), espace, alimentation.

L'article 14 de la directive (UE) 2022/2557 du Parlement européen et du Conseil (REC), prévoit que : « 1. Les États membres précisent les conditions dans lesquelles une entité critique est autorisée, dans des cas dûment motivés et compte tenu de l'évaluation des risques d'État membre, à présenter des demandes de vérification des antécédents (…) ».

Cette vérification concerne trois catégories de personnes :

- Celles exerçant des fonctions considérées comme sensibles pour l'opérateur ;
- Celles qui accèdent physiquement ou à distance aux PIV ou aux systèmes d'information ;
- Celles pour lesquelles un recrutement est envisagé sur un poste sensible.

1.4. ÉLEMENTS DE DROIT COMPARE

Plusieurs Etats membres, notamment la Belgique, disposent de dispositifs comparables au système actuellement en vigueur en France.

2. NECESSITE DE LEGIFERER ET OBJECTIFS POURSUIVIS

2.1. NECESSITE DE LEGIFERER

L'article 14 de la directive REC demande aux Etats membres de « prévoir les conditions dans lesquelles une entité critique est autorisée, dans des cas dûment motivés et compte tenu de l'évaluation des risques d'Etat membre, à présenter des demandes de vérification des antécédents des personnes ». Ces enquêtes doivent pouvoir porter sur un champ plus large que le cadre français actuel, à savoir sur :

- les personnes qui occupent des fonctions sensibles au sein de l'opérateur d'importance vitale ou pour le compte de celui-ci, notamment en ce qui concerne la résilience de l'entité ;

- les personnes ayant accès à distance aux locaux et aux systèmes d'informations ou de contrôle de l'opérateur, y compris en lien avec sa sécurité ;
- les personnes dont le recrutement est envisagé à des postes répondant aux critères énoncés aux points précédents.

La directive REC prévoit également un certain nombre de conditions dans le traitement de ces demandes. Les Etats membres doivent en effet traiter ces demandes dans un délai « raisonnable », de manière conforme au droit national et aux procédures nationales, ainsi qu'au droit de l'Union européenne. Ces demandes doivent être « *proportionnées et strictement limitées à ce qui est nécessaire. Elles sont effectuées dans le seul but d'évaluer un risque potentiel pour la sécurité de l'entité […] concernée* » (paragraphe 2 de l'article 14 de la directive « REC »). Ces demandes doivent *a minima* corroborer l'identité de la personne faisant l'objet d'une demande de « criblage » et vérifier les casiers judiciaires de ladite personne.

Au vu de ces éléments et de la possibilité donnée à des opérateurs, publics comme privés, de demander la réalisation d'enquêtes administratives de sécurité au regard de leur statut d'opérateur d'importance vitale, il apparait indispensable de cadrer ces dispositions au niveau législatif, puis de les décliner au niveau réglementaire afin d'offrir les garanties nécessaires aux individus qui pourraient faire l'objet de telles enquêtes. L'article 34 de la Constitution réserve en effet à la loi le soin de fixer les règles en matière d'organisation de la Défense nationale et d'exercice des libertés publiques.

2.2. OBJECTIFS POURSUIVIS

Les dispositions proposées visent à la fois à mettre en cohérence le dispositif avec le nouveau champ prévu par la directive (accès à distance et fonctions sensibles) et avec l'avis du Conseil d'Etat susmentionné.

3. OPTIONS ENVISAGEES ET DISPOSITIF RETENU

3.1. OPTIONS ENVISAGEES

Sans objet.

3.2. DISPOSITIF RETENU

Le dispositif retenu prévoit l'élargissement du champ des enquêtes administratives de sécurité aux accès à distance aux PIV, ainsi qu'aux fonctions sensibles, conformément à la directive. Il

acte également le passage à un avis conforme lorsque celui-ci est négatif et demandé par une personne privée, pour tenir compte de l'avis susmentionné.

4. ANALYSE DES IMPACTS DES DISPOSITIONS ENVISAGEES

4.1. IMPACTS JURIDIQUES

4.1.1. Impact sur l'ordre juridique interne

La présente mesure remplace l'article L. 1332-6 du code de la défense, désormais consacré au cadre des enquêtes administratives de sécurité pour l'accès aux PIV, qui figurait à l'article L. 1332-2-1 du même code.

De telles dispositions portent atteinte à la liberté d'entreprendre, à la liberté de circulation et au droit d'obtenir un emploi. Ces atteintes sont toutefois proportionnées et justifiées par des motifs liés à l'ordre public et à la défense nationale. Par ailleurs, cette atteinte se concilie avec le droit de chacun d'obtenir un emploi.

4.1.2. Articulation avec le droit international et le droit de l'Union européenne

Les dispositions de la présente mesure s'inscrivent dans le champ de la transposition de la directive européenne sur la résilience des entités critiques du (REC) du 14 décembre 2022, notamment son article 14.

4.2. IMPACTS ECONOMIQUES ET FINANCIERS

4.2.1. Impacts macroéconomiques

Les mesures de résilience prévues pourront engendrer des coûts supplémentaires pour un opérateur. Si la logique de protection physique était déjà prise en compte, la systématisation de la prise en compte de la continuité d'activité ne sera en effet pas neutre. Ces coûts sont extrêmement difficiles à évaluer tant les opérateurs de la SAIV opèrent dans des secteurs diversifiés et à différentes échelles.

Néanmoins, le principe de résilience – au cœur de cette transposition – permettra *in fine* à l'opérateur et – au regard de certaines dépendances – à l'ensemble du tissu économique de pouvoir maintenir son activité dans un contexte dégradé et vise à amortir les coûts imputables à la disruption de son activité.

4.2.2. Impacts sur les entreprises

Les opérateurs pourront solliciter des enquêtes sur un champ plus large, afin de renforcer leur sécurité. Ils ne pourront toutefois plus déroger aux avis défavorables, dès lors que l'entité dispose d'un statut privé, conformément à l'avis du Conseil d'Etat susmentionné.

4.2.3. Impacts budgétaires

L'élargissement du champ des enquêtes pourrait avoir une incidence sur le volume d'enquêtes réalisées, nécessitant un renforcement en ressources humaines des services enquêteurs concernés.

4.3. IMPACTS SUR LES COLLECTIVITES TERRITORIALES

Sans objet.

4.4. IMPACTS SUR LES SERVICES ADMINISTRATIFS

Comme évoqué supra, l'élargissement du champ des enquêtes pourrait avoir une incidence sur le volume d'enquêtes réalisées, nécessitant un renforcement en ressources humaines des services enquêteurs concernés : le Service National des Enquêtes Administratives de Sécurité (SNEAS), la Direction du renseignement et de la sécurité de la défense, et le Commandement spécialisé pour la sécurité nucléaire (CoSSeN).

4.5. IMPACTS SOCIAUX

4.5.1. Impacts sur la société

Le renforcement des exigences en matière de sécurité des activités d'importance vitale doit permettre de limiter les impacts d'une crise ou de problèmes majeurs d'un opérateur d'importance vitale sur le fonctionnement de la société.

4.5.2. Impact sur les personnes en situation en handicap

Sans objet.

4.5.3. Impacts sur l'égalité entre les femmes et les hommes

Sans objet.

4.5.4. Impacts sur la jeunesse

Sans objet.

4.5.5. Impacts sur les professions réglementées

Sans objet.

4.6. IMPACTS SUR LES PARTICULIERS

Les modalités de réalisation des enquêtes demeurent inchangées. Seul le périmètre des enquêtes est élargi.

4.7. IMPACTS ENVIRONNEMENTAUX

Sans objet.

5. CONSULTATIONS MENEES ET MODALITES D'APPLICATION

5.1. CONSULTATIONS MENEES

Une concertation de l'ensemble des ministères coordonnateurs a été réalisée sur cette mesure.

En application de l'article L. 1212-2 du code général des collectivités territoriales, le présent article a été soumis à l'examen du Conseil national d'évaluation des normes qui a rendu un avis défavorable le 22 mai 2024.

Enfin, le service national des enquêtes administratives de sécurité, le coordinateur général de la sécurité nucléaire, le service juridique du Secrétariat général des affaires européennes et l'Agence nationale de sécurité des systèmes d'informations ont également été consultés.

5.2. MODALITES D'APPLICATION

5.2.1. Application dans le temps

Les présentes dispositions entrent en vigueur le lendemain de la publication de la présente loi au *Journal officiel* de la République française.

5.2.2. Application dans l'espace

Le présent article est applicable de plein droit sur l'ensemble du territoire de la République conformément à l'article L. 1 du code de la défense.

Aussi, les dispositions du code de la défense créées par le présent projet de loi seront applicables de plein droit à la fois dans les collectivités régies par le principe de l'identité législative (la Guadeloupe, la Guyane, la Martinique, La Réunion, Mayotte, Saint-Barthélemy, Saint-Martin et Saint-Pierre-et-Miquelon) et par le principe de la spécialité législative (les îles Wallis et Futuna, la Polynésie française, la Nouvelle-Calédonie et les Terres australes et antarctiques françaises).

En tant que PTOM, le droit de l'union européenne ne s'applique pas à Saint-Barthélemy, Saint-Pierre-et-Miquelon, dans les îles Wallis et Futuna, en Polynésie française, Nouvelle-Calédonie et dans les Terres australes et antarctiques françaises. Les dispositions applicables aux seuls OIV exerçant des services essentiels au fonctionnement du marché intérieur de l'Union européenne ne seront donc pas applicables en l'absence d'adaptation.

5.2.3. Textes d'application

Le présent article, à l'instar des autres dispositions législatives du Titre I du présent projet de loi, fera l'objet d'un décret en Conseil d'Etat afin de préciser les modalités et les cas de saisine d'une demande d'enquête administrative.

Article 1er (G) – Article L. 1332-7 du code de la défense – Notification d'incidents

1. ETAT DES LIEUX

1.1. CADRE GENERAL

Notification des incidents physiques

Le dispositif de sécurité des activités d'importance vitale actuel ne comprend pas aujourd'hui d'obligation pour les opérateurs d'importance vitale de réaliser des notifications d'incidents physiques auprès de l'autorité administrative.

Si l'obligation de notifier les incidents auprès de l'autorité administrative ne figure pas dans la loi, il est tout de même demandé aux opérateurs d'avoir une vision de leurs incidents : l'Instruction générale interministérielle n°6600 relative la sécurité des activités d'importance vitale[51] (IGI 6600), adoptée en 2014, rappelle bien dans la partie « Révision du PPP » (3.5.3, p. 31) que l'opérateur peut être tenu de réviser son plan particulier de protection dans plusieurs cas, y compris « *en cas de modification des conditions d'exploitation du PIV ou de certaines données d'environnement (urbanisation, augmentation de la délinquance, incidents de sûreté, etc.)* ». Le document mentionne également les incidents de sécurité répertoriés comme des « *données intéressantes au titre de la sécurité du site* »[52] pouvant être communiquées par l'opérateur en amont d'une visite de contrôle. Enfin, ces incidents sont également mentionnés dans la trame de rapport d'incident indiquée dans l'annexe 7[53] de l'IGI 6600.

Le suivi des incidents de l'opérateur d'importance vitale sur ses sites est également sous-entendu dans le guide pour l'élaboration d'un plan de sécurité d'opérateur paru en 2018. Les opérateurs, lors de l'élaboration de leur plan de sécurité opérateur (PSO), sont tenus de développer des éléments de leur dispositif d'alerte et de gestion de crise[54], qui comprend une partie portant sur la gestion de l'alerte. L'opérateur est donc tenu, dans sa planification qui est aujourd'hui revue par l'autorité administrative, de décrire son schéma d'alerte, de gestion des astreintes et de remontée d'incidents. Au niveau local, les points d'importance vitale sont

[51] https://www.legifrance.gouv.fr/circulaire/id/37828.

[52] IGI 6600, Partie 4 « Audit et Contrôle », section 4.3.2 « Préparation du contrôle sur place ».

[53] IGI 6600, Annexe 7 établissant un modèle de rapport de contrôle d'un point d'importance vitale par une commission de défense et de sécurité des secteurs d'activité d'importance vitale.

[54] Partie 2.5 du Guide pour l'élaboration d'un plan de sécurité d'opérateur de 2018.

tenus, dans leur plan particulier de protection (PPP)[55], de prévoir une remontée d'informations avec plusieurs entités, à savoir les autorités de décision interne, les autorités administratives (services préfectoraux, forces de sécurité intérieure, service du haut fonctionnaire de défense et de sécurité du ministère coordonnateur) ainsi que les populations et abonnés prioritaires si nécessaire.

De surcroît, les opérateurs peuvent avoir à remonter certains types d'incidents à l'autorité administrative, du fait de règlementations autres que celle relative à la sécurité des activités d'importance vitale. A titre d'exemple, les opérateurs désignés au titre du secteur des transports maritimes peuvent être tenus de remonter certains incidents qui pourraient avoir lieu sur leur site au titre de la règlementation résultant du Code international pour la sûreté des navires et des installations portuaires[56]. C'est également le cas pour les opérateurs relevant du secteur des télécommunications au titre des dispositions en vigueur du Code des postes et des télécommunications électroniques[57].

Notification des incidents de cybersécurité

Les opérateurs d'importance vitale doivent, en application de l'article L. 1332-6-2 du code de la défense, notifier au Premier ministre les incidents qui affecteraient le fonctionnement des systèmes d'informations d'importance vitale (SIIV) qu'il a pu désigner au titre du L. 1332-6-1 du code de la défense. Cette obligation a été intégrée au dispositif en 2013, avec l'adoption 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 qui a créé le statut des systèmes d'informations d'importance vitale (SIIV).

Ces incidents, qui relèvent avant tout de la cybersécurité, sont dans les faits notifiés

- à l'Agence nationale de sécurité des systèmes d'informations (ANSSI), via le CERT-FR ;
- ou au ministre de la défense, en application du décret n° 2024-158 du 28 février 2024 relatif à la sécurité des systèmes d'information d'importance vitale relevant du contrôle gouvernemental de la dissuasion nucléaire ;

[55] Partie 6 Procédure d'alerte et de gestion de crise du Guide d'aide à l'élaboration et l'examen d'un plan particulier de protection de 2018.

[56] Arrêté du 11 août 2016 fixant les règles de sécurité et les modalités de déclaration des systèmes d'information d'importance vitale et des incidents de sécurité relatives au secteur d'activités d'importance vitale « Transports maritime et fluvial » et 20220628-sgdsn-pse-psn-np-iim-230-relative-a-lorganisation-et-a-la-coordination-de-la-surete-maritime-et-portuaire.pdf.

[57] Article D. 98-5 du code des postes et communications électroniques et Guide pour la déclaration des incidents affectant les réseaux et infrastructures de communications électroniques et de l'internet ouverts au public (entreprises.gouv.fr).

- ou au ministre de la défense pour ceux qui concernent la protection et le contrôle des matières nucléaires, de leurs installations, et de leurs transports qui relèvent de sa compétence ;
- à l'ANSSI, via le CERT-FR et au ministre de la transition écologique et de la cohésion des territoires pour ceux qui concernent la protection et le contrôle des matières nucléaires, de leurs installations, et de leurs transports qui relèvent de sa compétence ;
- à l'ANSSI, via le CERT-FR et au ministre de la transition écologique et de la cohésion des territoires pour ceux qui concernent la sécurité et sûreté de l'aviation civile.

L'ANSSI effectue la détection et la supervision pour les services. Le service est en charge de la coopération au niveau national et international. A ce titre, il anime un écosystème de relais au niveau ministériel et régional. Le but de ces relais régionaux ou ministériels est de sensibiliser des acteurs qui ne traitent pas de manière directe avec l'ANSSI.

Les notifications d'incidents effectuées à l'autorité nationale de sécurité des systèmes d'information et, le cas échéant, à l'ANSSI peuvent faire l'objet d'une réaction ou assistance opérationnelle de la part de l'agence ou de l'autorité. En effet, l'autorité nationale est tenue d'effectuer, sur la base du signalement effectué par l'entité, des recommandations à la suite d'un incident. La remontée d'information effectuée peut donc générer une réponse opérationnelle. Les informations remontées à l'autorité nationale de sécurité des systèmes d'information concernent :

- Tout incident qui impacterait la continuité de service de l'entité ;
- Tout incident qui impacterait un vol d'informations ;
- D'autres incidents pour lesquels il est jugé utile d'effectuer une remontée d'informations.

L'enjeu de cette remontée d'informations est d'avoir mis un certain nombre de critères en amont de la saisine de l'opérateur, afin d'obtenir des informations pertinentes, pouvant être traitées dans un laps de temps restreint.

Actuellement, les opérateurs peuvent saisir l'autorité nationale de sécurité des systèmes d'information d'un incident cyber par plusieurs canaux de remontée d'informations – formulaire, courriel, appel téléphonique, courrier papier pour les informations sensibles, etc. Le déclarant rapporte son incident, et une prise de contact est faite rapidement suivant la demande de précisions – que ce soit pour répondre à une demande d'assistance ou pour capitaliser sur les données. Il n'y a pas de réponse automatique, mais il existe des fiches réflexes ou procédures à utiliser suivant les situations – par exemple, il est rappelé à l'opérateur de faire une déclaration à la CNIL en cas de perte de données clients ou de déposer plainte. Un rappel des aides existantes peut également être effectué, ainsi que des conseils sur la communication que l'opérateur peut avoir auprès de son personnel comme de ses clients. L'opérateur indique en général s'il s'agit d'une notification obligatoire. L'autorité

nationale de sécurité des systèmes d'information qualifie l'importance de l'incident. La remontée peut donc s'effectuer en deux temps : une primo-notification, effectuée de manière rapide, puis une demande à l'opérateur de produire un rapport plus approfondi via un formulaire à remplir.

1.2. CADRE CONSTITUTIONNEL

Le cadre constitutionnel le respect d'une exigence constitutionnelle de transposition des directives européennes et d'atteinte justifiée et proportionnée à la liberté d'entreprendre compte tenu des sujétions imposées aux opérateurs.

Aux termes de l'article 88-1 de la Constitution : « La République participe aux Communautés européennes et à l'Union européenne, constituées d'Etats qui ont choisi librement, en vertu des traités qui les ont instituées, d'exercer en commun certaines de leurs compétences ». Le Conseil constitutionnel déduit de cette disposition que : « la transposition en droit interne d'une directive communautaire résulte d'une exigence constitutionnelle »[58]. Il en va de même pour une loi ayant pour objet d'adapter le droit interne à un règlement de l'Union européenne[59].

L'obligation de notification des incident à l'autorité administrative, à la charge des OIV, porte nécessairement une atteinte à la liberté d'entreprendre, laquelle découle de l'article 4 de la Déclaration des droits de l'Homme et du Citoyen de 1789[60]. Cette atteinte ne peut être ni générale ni absolue[61]. Le législateur peut limiter l'exercice de cette liberté à la condition qu'il n'en résulte pas d'atteintes disproportionnées au regard de l'objectif poursuivi[62], alors même que cette atteinte résulterait de l'exigence constitutionnelle de transposition adéquate des directives européennes[63], dans un objectif de sécurité et de défense de la Nation, en l'absence de disposition spécifique contraire de la Constitution[64] ou de mise en cause d'une règle ou d'un principe inhérent à notre identité constitutionnelle[65].

[58] voir notamment la décision n° 2004-496 DC du 10 juin 2004, « Loi pour la confiance dans l'économie numérique ».

[59] voir par exemple la décision n° 2018-765, « Loi relative à la protection des données personnelles », considérant 3.

[60] Conseil constitutionnel, décision 98-401 DC du 10 juin 1998.

[61] Décision 82-141 DC du 27 juillet 1982.

[62] Décision 2023-1055 QPC du 16 juin 2023.

[63] Décision 2006-535 DC du 30 mars 2006.

[64] Décision 2004-497 DC du 1er juillet 2004.

[65] Décision 2018-765 DC du 12 juin 2018 ; décision 2019-818 QPC du 6 décembre 2019.

Enfin, en l'absence de remise en cause de ses garanties fondamentales, la liberté du commerce et de l'industrie ne s'oppose pas à l'intervention du législateur dans ce domaine[66].

1.3. CADRE CONVENTIONNEL

Au niveau européen, la directive (UE) 2022/2557 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience des entités critiques (REC) permet désormais d'offrir un socle minimal commun de résilience à tous les opérateurs de l'UE. Elle doit être transposée dans notre droit national d'ici le 17 octobre 2024.

Son champ d'application couvre 11 secteurs : énergie, transports, infrastructures bancaires, infrastructures de marché financier, santé, eau potable, assainissement, infrastructures digitales, administration publique (niveau central), espace, alimentation.

L'article 14 de la directive consacre l'obligation pour les opérateurs d'effectuer une notification de leurs incidents à l'autorité administrative. Les Etats membres doivent en effet être capables d'obtenir les informations reçues, de les traiter, de fournir à l'entité des informations pouvant l'aider à la résolution de l'incident et de prévenir les autres Etats membres et la Commission si l'incident en question est susceptible de les concerner.

L'article 15 de la directive insiste sur l'importance que ces incidents soient notifiés « *sans retard injustifié* » : ceux-ci doivent faire l'objet d'une première notification dans les 24h et être suivie, dans le mois qui suit l'incident, par un rapport détaillé partagé par l'entité auprès de son autorité.

Les opérateurs identifiés comme entités critiques par l'Etat membre doivent notifier à autorité administrative « *les incidents qui perturbent ou sont susceptibles de perturber de manière importante la fourniture de services essentiels* ». Les opérateurs auront donc à évaluer non seulement l'impact mais également les impacts possibles que pourraient avoir l'incident.

Plusieurs critères d'impact sont mis en avant dans le texte de la directive, à savoir :

- le nombre et la proportion d'utilisateurs affectés par la perturbation ;
- la durée de la perturbation ;
- la zone géographique concernée par la perturbation, en tenant compte de son éventuel isolement géographique.

La directive statue également sur le minimum d'informations que devra fournir les notifications d'incidents et le rapport détaillé d'incident, en indiquant que ces informations doivent permettre à l'autorité compétente de saisir la « *nature, la cause et les conséquences*

[66] Décision 2003-474 DC du 17 juillet 2003.

possibles de l'incident, y compris toute information disponible nécessaire pour déterminer tout impact transfrontière de l'incident ».

1.4. ÉLEMENTS DE DROIT COMPARE

Sans objet.

2. NECESSITE DE LEGIFERER ET OBJECTIFS POURSUIVIS

2.1. NECESSITE DE LEGIFERER

Les critères et modalités de la procédure de remontée d'incidents mentionnés aux articles 14 et 15 de la directive REC, qui doivent être adaptées pour tous les secteurs d'activités, devront être spécifiées au niveau infra-réglementaire et explicitées dans les directives nationales de sécurité (DNS). Une prise en compte des particularités des territoires ultramarins devra également être prise en compte, par exemple en identifiant des critères de remontée d'incidents pouvant être différents mais plus pertinents au regard des caractéristiques de ces territoires. L'ensemble de ces dispositions réglementaires ou infra-réglementaires nécessitent donc un cadre législatif clair. L'article 34 de la Constitution impose de recourir à la loi s'agissant d'une mesure d'organisation de la défense nationale laquelle impose des sujétions à des opérateurs qui peuvent être des collectivités territoriales ou des opérateurs privés.

Enfin, la directive dispose également que les Etats membres informent le public desdits incidents « *lorsqu'ils estiment qu'il serait dans l'intérêt général de le faire* ». Cette disposition, qui est une option laissée à l'appréciation des Etats membres, doit figurer dans le projet de loi.

2.2. OBJECTIFS POURSUIVIS

Les dispositions prévues visent à instaurer le régime de notification d'incidents requis par la directive. En raison des différences sectorielles, il ne peut fixer de manière précise l'ensemble des critères qui pourraient être identifiés par l'entité avant de notifier son incident, il s'attache donc à ce que l'opérateur remonte tout incident qui pourrait affecter son activité d'importance vitale – activité qui est à l'origine même de sa désignation.

A terme, l'objectif de cette nouvelle obligation pour les opérateurs est que le nouveau dispositif de notification d'incident soit adapté à chaque secteur d'activité, par l'identification de critères qui seraient fixés dans les directives nationales de sécurité et via les canaux d'informations et les acteurs idoines. Des critères communs pourraient également être identifiés entre les différents secteurs, en particulier lorsque les incidents ont des origines

malveillantes. Cette remontée d'informations devra se faire *via* les canaux d'informations idoines : certaines informations fournies par les opérateurs pourraient avoir à être protégées par le secret de la défense nationale, ou avec des procédures permettant cette protection.

3. OPTIONS ENVISAGEES ET DISPOSITIF RETENU

3.1. OPTIONS ENVISAGEES

Comme indiqué au point 2.2, certaines informations fournies par les opérateurs pourraient avoir à être protégées par le secret de la défense nationale, ou avec des procédures permettant cette protection, rendant l'information au public très limitée.

3.2. DISPOSITIF RETENU

Le premier alinéa de l'article fixe l'obligation de notification d'incidents à l'autorité administrative, dans un délai prévu par décret en Conseil d'Etat. Le second exige de l'autorité administrative compétente qu'elle informe le public lorsqu'il est dans l'intérêt général de le faire.

4. ANALYSE DES IMPACTS DES DISPOSITIONS ENVISAGEES

4.1. IMPACTS JURIDIQUES

4.1.1. Impact sur l'ordre juridique interne

La présente disposition remplace l'article L. 1332-7 du code de la défense.

La mesure est une nouvelle obligation juridique pour le dispositif de sécurité des activités d'importance vitale. Les obligations seront complétées au niveau réglementaire puis dans les documents cadres du dispositif SAIV, les directives nationales de sécurité dont les missions et contenus seront explicitées dans le cadre réglementaire – comme c'est le cas dans le dispositif actuel.

Il faudra que les obligations de remontée d'informations prennent en compte les obligations pouvant exister pour certains secteurs sur ce sujet, par exemple pour le secteur des télécommunications qui peut être concerné par l'obligation réglementaire instaurée par l'article D. 98-5 du Code des postes et des communications électroniques.

4.1.2. Articulation avec le droit international et le droit de l'Union européenne

Les dispositions de la présente mesure s'inscrivent dans le champ de la transposition de la directive européenne sur la résilience des entités critiques du (REC) du 14 décembre 2022, notamment son article 15.

4.2. IMPACTS ECONOMIQUES ET FINANCIERS

4.2.1. Impacts macroéconomiques

Sans objet.

4.2.2. Impacts sur les entreprises

Le nouveau dispositif implique pour l'opérateur d'identifier dans sa planification un schéma d'alerte et de notifications d'incidents avec l'autorité administrative compétente. Il devra également mettre en œuvre ce schéma d'alerte et de gestion de crise au sein de chaque site identifié comme point d'importance vitale.

Cela s'intègre dans les coûts des mesures de résilience prévues par l'opérateur, ainsi que dans la réalisation de ses documents de planification.

4.2.3. Impacts budgétaires

Sans objet.

4.3. IMPACTS SUR LES COLLECTIVITES TERRITORIALES

Les collectivités territoriales désignées comme opérateurs continueront, comme ils l'ont fait jusqu'à présent, à assumer à leurs frais les mesures indispensables à leur résilience. Comme indiqué dans la partie 4.2.2, cette obligation sera intégrée dans la planification des opérateurs, qui devra prévoir un schéma d'alerte et de gestion de crise afin de gérer au mieux l'incident.

4.4. IMPACTS SUR LES SERVICES ADMINISTRATIFS

L'impact sur les services administratifs sera dimensionnant :

- Au niveau territorial, les préfectures ainsi que les zones de défense devront être notifiées des incidents afin de pouvoir réagir en tant que de besoin – via s'il le faut une intervention des forces de sécurité intérieure mais aussi afin d'avoir une connaissance des enjeux de leur territoire ;

- Au niveau national, un suivi par les ministères coordonnateurs ainsi que par le SGDSN sera effectué afin d'identifier rapidement les incidents pouvant avoir des incidences majeures sur la continuité d'activité des activités d'importance vitale, prévoir les mesures de réaction nécessaires et avoir un état des lieux de la malveillance ou de la menace pouvant affecter le dispositif.

Ce suivi nécessitera la mise en place de cellules opérationnelles ou d'astreinte. Un suivi des incidents devra être effectué et une analyse des conséquences desdits incidents devra être produite. Ce traitement de l'information remontée demandera un suivi de la part des différentes autorités en charge du suivi du dispositif. La fourniture d'informations aux opérateurs d'importance vitale de même qu'aux services de renseignement devra être prévue.

Pour les ministères, si certains disposaient déjà de cellules d'astreinte voire de centres opérationnels, ce n'est pas le cas de tous. Un renforcement en ressources humaines sera donc à prévoir pour les services impactés (centres de crises des ministères), afin de s'assurer que le traitement de l'information devant être fournie par l'opérateur dans les 24h soit effectué dans des délais raisonnable et qu'une possible réaction soit prévue rapidement.

4.5. IMPACTS SOCIAUX

4.5.1. Impacts sur la société

Le renforcement des exigences en matière de sécurité des activités d'importance vitale doit permettre de limiter les impacts d'une crise ou de problèmes majeurs d'un opérateur d'importance vitale sur le fonctionnement de la société.

4.5.2. Impact sur les personnes en situation en handicap

Sans objet.

4.5.3. Impacts sur l'égalité entre les femmes et les hommes

Sans objet.

4.5.4. Impacts sur la jeunesse

Sans objet.

4.5.5. Impacts sur les professions réglementées

Sans objet.

4.6. IMPACTS SUR LES PARTICULIERS

Sans objet.

4.7. IMPACTS ENVIRONNEMENTAUX

Sans objet.

5. CONSULTATIONS MENEES ET MODALITES D'APPLICATION

5.1. CONSULTATIONS MENEES

Une concertation de l'ensemble des ministères coordonnateurs a été réalisée sur cette mesure.

En application de l'article L. 1212-2 du code général des collectivités territoriales, le présent article a été soumis à l'examen du Conseil national d'évaluation des normes qui a rendu un avis défavorable le 22 mai 2024.

Enfin, le service national des enquêtes administratives de sécurité, le coordinateur général de la sécurité nucléaire, le service juridique du Secrétariat général des affaires européennes et l'Agence nationale de sécurité des systèmes d'informations ont également été consultés.

5.2. MODALITES D'APPLICATION

5.2.1. Application dans le temps

Les présentes dispositions entrent en vigueur le lendemain de la publication de la présente loi au *Journal officiel* de la République française.

5.2.2. Application dans l'espace

Le présent article est applicable de plein droit sur l'ensemble du territoire de la République conformément à l'article L. 1 du code de la défense.

Aussi, les dispositions du code de la défense créées par le présent projet de loi seront applicables de plein droit à la fois dans les collectivités régies par le principe de l'identité législative (la Guadeloupe, la Guyane, la Martinique, La Réunion, Mayotte, Saint-Barthélemy, Saint-Martin et Saint-Pierre-et-Miquelon) et par le principe de la spécialité législative (les îles Wallis et Futuna, la Polynésie française, la Nouvelle-Calédonie et les Terres australes et antarctiques françaises).

En tant que PTOM, le droit de l'union européenne ne s'applique pas à Saint-Barthélemy, Saint-Pierre-et-Miquelon, dans les îles Wallis et Futuna, en Polynésie française, Nouvelle-Calédonie et dans les Terres australes et antarctiques françaises. Les dispositions applicables aux seuls OIV exerçant des services essentiels au fonctionnement du marché intérieur de l'Union européenne ne seront donc pas applicables en l'absence d'adaptation.

5.2.3. Textes d'application

Le présent article, à l'instar des autres dispositions législatives du Titre I du présent projet de loi, fera l'objet d'un décret en Conseil d'Etat afin de préciser la procédure de notification des incidents ainsi que le délai dans lequel cette notification doit intervenir.

Article 1er (H) – Articles L. 1332-8 et 9 du code de la défense – Dispositions applicables aux entités critiques d'importance européenne particulière

1. ETAT DES LIEUX

1.1. CADRE GENERAL

Présentation de la directive sur les infrastructures critiques européenne de 2008

A la suite des attentats de Madrid en 2004 et Londres en 2005 dans les transports, les Etats membres de l'Union européenne ont ouvert des discussions et échanges portant sur la résilience des infrastructures critiques au niveau européen. Le programme européen de protection des infrastructures critiques (PEPIC) a été adopté en 2006[67]. Les menaces auxquelles il doit répondre ne se limitaient pas seulement au terrorisme, mais englobaient les activités criminelles, les catastrophes naturelles et d'autres causes d'accidents, selon une approche tous risques. L'objectif général était d'améliorer la protection des infrastructures critiques dans l'Union européenne. C'est dans ce cadre qu'a été adoptée la directive 2008/114/CE du Conseil du 8 décembre 2008 concernant le recensement et la désignation des infrastructures critiques européennes ainsi que l'évaluation de la nécessité d'améliorer leur protection[68]. Cette directive, abrogée par la directive (UE) 2022/2557 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience des entités critiques (REC), prévoyait un mécanisme d'identification et de désignation des infrastructures critiques européennes (ICE) « *dont l'arrêt ou la destruction aurait un impact considérable sur deux Etats membres au moins* », dans les seuls secteurs des transports et de l'énergie. La mise en œuvre de ce mécanisme s'appuyait sur des lignes directrices (non contraignantes) élaborées conjointement par la Commission et les Etats membres, et reposait donc essentiellement sur la coopération entre Etats membres, sur une base volontaire.

La directive REC prévoit un niveau de coopération et d'harmonisation supérieur à la directive de 2008 en :

- prévoyant un cadre minimal commun pour l'ensemble des entités critiques nationales des Etats membres, pour l'ensemble des secteurs concourant au fonctionnement du marché intérieur ;

[67] COM(2006) 786 final – Journal officiel C 126 du 7 juin 2007.

[68] https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32008L0114.

- conservant un volet de coopération européenne entre les Etats membres ainsi qu'avec la Commission européenne via notamment la création du statut spécifique d'entité critique d'importance européenne particulière.

1.2. CADRE CONSTITUTIONNEL

Les dispositions proposées résultent directement de la transposition de la directive REC qui prévoit des dispositions spécifiques pour certains opérateurs lorsqu'ils ont un intérêt au niveau de plusieurs Etats membres.

Aux termes de l'article 88-1 de la Constitution : « La République participe aux Communautés européennes et à l'Union européenne, constituées d'Etats qui ont choisi librement, en vertu des traités qui les ont instituées, d'exercer en commun certaines de leurs compétences ». Le Conseil constitutionnel déduit de cette disposition que : « la transposition en droit interne d'une directive communautaire résulte d'une exigence constitutionnelle »[69]. Il en va de même pour une loi ayant pour objet d'adapter le droit interne à un règlement de l'Union européenne[70].

Les dispositions applicables aux entités critiques d'importance européenne particulière portent nécessairement une atteinte à la liberté d'entreprendre, laquelle découle de l'article 4 de la Déclaration des droits de l'Homme et du Citoyen de 1789[71]. Cette atteinte ne peut être ni générale ni absolue[72]. Le législateur peut limiter l'exercice de cette liberté à la condition qu'il n'en résulte pas d'atteintes disproportionnées au regard de l'objectif poursuivi[73], alors même que cette atteinte résulterait de l'exigence constitutionnelle de transposition adéquate des directives européennes[74], dans un objectif de sécurité et de défense de la Nation, en l'absence de disposition spécifique contraire de la Constitution[75] ou de mise en cause d'une règle ou d'un principe inhérent à notre identité constitutionnelle[76].

[69] Voir notamment la décision n° 2004-496 DC du 10 juin 2004, « Loi pour la confiance dans l'économie numérique ».

[70] Voir par exemple la décision n° 2018-765, « Loi relative à la protection des données personnelles », considérant 3.

[71] Conseil constitutionnel, décision 98-401 DC du 10 juin 1998.

[72] Décision 82-141 DC du 27 juillet 1982.

[73] Décision 2023-1055 QPC du 16 juin 2023.

[74] Décision 2006-535 DC du 30 mars 2006.

[75] Décision 2004-497 DC du 1er juillet 2004.

[76] Décision 2018-765 DC du 12 juin 2018 ; décision 2019-818 QPC du 6 décembre 2019.

Enfin, en l'absence de remise en cause de ses garanties fondamentales, la liberté du commerce et de l'industrie ne s'oppose pas à l'intervention du législateur dans ce domaine[77].

1.3. CADRE CONVENTIONNEL

Au niveau européen, la directive (UE) 2022/2557 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience des entités critiques (REC) permet désormais d'offrir un socle minimal commun de résilience à tous les opérateurs de l'UE. Elle doit être transposée dans notre droit national d'ici le 17 octobre 2024.

Son champ d'application couvre 11 secteurs : énergie, transports, infrastructures bancaires, infrastructures de marché financier, santé, eau potable, assainissement, infrastructures digitales, administration publique (niveau central), espace, alimentation.

Le chapitre IV de la directive traite des entités critiques d'importance européenne particulière.

L'article 17 de la directive crée une nouvelle catégorie d'entités considérées comme critiques au niveau européen, les « entités critiques d'importance européenne particulière », pour lesquelles la directive impose des obligations supplémentaires. Un statut spécifique pour ces entités soumises à des obligations particulières doit donc figurer dans la loi.

L'identification des entités critiques d'importance européenne particulière doit répondre à plusieurs conditions énumérées par l'article 17 de la directive :

- l'entité doit avoir été désignée en tant qu'entité critique – en France, cela sera nécessairement un opérateur d'importance vitale -,
- l'entité doit fournir les mêmes services essentiels ou des services essentiels similaires dans au moins six Etats membres ;
- l'entité a fait l'objet d'une notification de la part de l'autorité administrative sur la base d'une instruction de la Commission européenne.

Après adoption du présent projet de loi, l'entité devra avoir été désignée au titre du 1° u I de l'article L. 1332-2 du code de la défense.

L'article 18 de la directive crée pour la Commission européenne et les Etats membres concernés directement par l'entité critique d'importance européenne particulière la possibilité de réaliser des « missions de conseil ». Ces missions doivent avoir pour objectif d'évaluer les mesures mises en place par l'entité et de vérifier que l'entité met en œuvre les obligations de résilience prévues dans la directive.

[77] Décision 2003-474 DC du 17 juillet 2003.

1.4. ELEMENTS DE DROIT COMPARE

Sans objet.

2. NECESSITE DE LEGIFERER ET OBJECTIFS POURSUIVIS

2.1. NECESSITE DE LEGIFERER

L'opérateur d'importance vitale relevant de la catégorie d'entité critique au niveau européen doit assurer une activité d'importance vitale et fournir des services essentiels au sens de la directive.

La liste de ces services essentiels est établie depuis le 25 juillet 2023 dans l'acte délégué adopté par la Commission européenne[78], qui permet d'identifier les services pour lesquels les Etats membres sont tenus d'effectuer leur analyse des risques en vertu de l'application de l'article 5 de la directive.

La liste des services en question doit donc être évoquée dans la loi, de même que la définition des services essentiels afin que l'identification des entités concernées par les obligations européennes soit rendue possible.

L'introduction de la mention des services essentiels dans la loi est impérative selon les règles de transposition en vigueur, d'autant plus que les autorités françaises seront tenues de s'assurer que les opérateurs d'importance vitale qu'elles désigneront au titre du futur L. 1332-2 soient en mesure d'indiquer s'ils assurent un ou plusieurs services essentiels dans d'autres Etats membres.

Dans le cas où six Etats membres ou plus seraient concernés, les autorités françaises devront notifier cette information à la Commission européenne. Cette obligation pour les autorités françaises implique qu'elles soient en mesure de fournir ces informations.

Par ailleurs, les missions de conseil prévues à l'article 18 de la directive ne peuvent être effectuées qu'avec l'accord des autorités étatiques compétentes, mais si elles ont lieu l'opérateur devra donner accès à ces « missions de conseil » et lui fournir les informations nécessaires prévues dans la directive. A la suite de son inspection, la « mission de conseil » doit fournir ses conclusions à la Commission européenne, l'Etat membre qui a désigné l'entité ainsi que les autres Etats membres pour lesquels l'entité critique d'importance européenne particulière fournit au moins un service essentiel.

[78] Règlement délégué (UE) 2023/2450 de la Commission du 25 juillet 2023 complétant la directive (UE) 2022/2557 du Parlement européen et du Conseil en établissant une liste de services essentiels.

2.2. OBJECTIFS POURSUIVIS

L'objectif poursuivi est de s'assurer que les entités concernées par l'acte délégué de la directive, car fournissant des services considérés comme essentiels, puissent être clairement identifiées lorsqu'elles fournissent les mêmes services essentiels ou des services essentiels similaires dans au moins six Etats membres.

Cela permet aussi de faire une différenciation entre les opérateurs d'importance vitale qui sont concernés par l'application de la directive, pour lesquels les autorités françaises seront tenues d'effectuer des remontées d'information auprès de la Commission européenne et les opérateurs exclus d'obligations strictement européennes ou de remontée d'information. Les opérateurs en question sont les opérateurs concernés par l'exclusion prévue au premier article de la directive résilience des entités critiques : les secteurs régaliens – activités militaires de l'Etat, activités civiles de l'Etat, activités judiciaires, mais aussi les opérateurs dont les secteurs ne figurent pas dans l'annexe de la directive REC ou son acte délégué, à savoir le nucléaire ainsi que l'industrie. Pour l'ensemble des opérateurs désignés au titre de ces secteurs, qui seront donc considérés comme opérateurs d'importance vitale en France, aucune transmission d'information ne sera à effectuer par les autorités françaises auprès des autres Etats membres ou de la Commission européenne.

3. OPTIONS ENVISAGEES ET DISPOSITIF RETENU

3.1. OPTION ENVISAGEE

Durant les travaux interministériels a été évoqué le fait de ne pas faire de distinctions entre les secteurs concernés par la directive REC et les autres secteurs existant déjà actuellement au sein du dispositif SAIV (activités civiles de l'Etat, activités militaires de l'Etat, activités judiciaires de l'Etat, industrie, nucléaire).

Toutefois, il est apparu comme important pour des questions de souveraineté nationale de faire une distinction claire au sein de la loi entre les opérateurs concernés par les transmissions d'informations auprès d'autres Etats membres ainsi que de la Commission, en particulier pour les opérateurs qui pourraient être concernés par plusieurs secteurs au titre de la SAIV. La possibilité pour la Commission européenne d'organiser des missions de conseil au sein d'opérateurs d'importance vitale opérant sur des secteurs concernés par la directive mais aussi régaliens est apparu comme un risque trop important d'un point de vue de souveraineté pour que l'exclusion ne soit pas directement rappelée dans la loi.

3.2. DISPOSITIF RETENU

Le nouvel article L. 1332-8 prévoit l'obligation, pour les opérateurs, d'informer l'autorité administrative lorsqu'ils fournissent des services essentiels dans six Etats membres ou plus, et prévoit leur régime de désignation en tant qu'entité critique d'importance européenne particulière. L'article L. 1332-9 prévoit les modalités relatives à l'exécution des missions de conseil de la Commission européenne pour ces opérateurs, incluant notamment la nécessité de l'accord préalable de l'autorité administrative.

4. ANALYSE DES IMPACTS DES DISPOSITIONS ENVISAGEES

4.1. IMPACTS JURIDIQUES

4.1.1. Impact sur l'ordre juridique interne

La présente mesure insère les nouveaux articles L. 1332-8 et L. 1332-9 du code de la défense au sein au sein du chapitre II consacré à la « Résilience des activités d'importance vitale ».

La création d'une sous-section dédiée intitulée « Dispositions applicables aux entités critiques d'importance européenne particulière » permet d'identifier les opérateurs d'importance vitale fournissant des services essentiels au sens de la directive pour six Etats membres ou plus et pouvant être de ce fait désignés entité critique d'importance européenne particulière.

4.1.2. Articulation avec le droit international et le droit de l'Union européenne

Les dispositions de la présente mesure s'inscrivent dans le champ de la transposition de la directive européenne sur la résilience des entités critiques du (REC) du 14 décembre 2022, notamment ses articles 17 et 18.

La Commission européenne désigne les entités critique d'importance européenne particulière. Les opérateurs peuvent alors faire l'objet d'une mission de conseil au titre de laquelle il doit garantir l'accès aux informations, systèmes et installations relatifs à la fourniture de leurs services essentiels qui sont nécessaires à l'exécution de cette mission de conseil, dans le respect des secrets protégés par la loi.

Sur le fondement des conclusions de la mission de conseil, l'opérateur se voit communiquer par la Commission européenne un avis sur le respect de ses obligations et, le cas échéant, sur les mesures qui pourraient être prises pour améliorer sa résilience.

4.2. IMPACTS ECONOMIQUES ET FINANCIERS

4.2.1. Impacts macroéconomiques

Sans objet.

4.2.2. Impacts sur les entreprises

Seules les entreprises disposant du statut d'opérateur d'importance vitale et qui fourniraient des services considérés comme essentiels au sens de l'acte délégué du 25 juillet 2023 sont concernées.

Les obligations d'accès possible en cas de mission de conseil pour les entités critiques d'importance européenne particulière et de transmission d'information sont relativement peu contraignantes. Les opérateurs au sein desquels seraient organisés des missions de conseil de la Commission pourraient avoir à mettre en place des mesures supplémentaires de résilience, mais ces mesures éventuelles seront dans tous les cas à déterminer avec les autorités administratives françaises. Elles viendraient en complément des mesures que les opérateurs doivent mettre en œuvre au titre de la première sous-section, soit avec un impact financier limité.

4.2.3. Impacts budgétaires

Sans objet.

4.3. IMPACTS SUR LES COLLECTIVITES TERRITORIALES

Seules les collectivités territoriales disposant du statut d'opérateur d'importance vitale, et qui fourniraient des services considérés comme essentiels au sens de l'acte délégué du 25 juillet 2023, sont concernés.

A l'instar d'entreprises disposant de ce statut, la nouvelle obligation créée par le présent article sera peu contraignante puisqu'elle consistera à prendre en compte le statut des opérateurs, à accorder un accès possible en cas de mission de conseil pour les entités critiques d'importance européenne particulière et à transmettre des informations supplémentaires si cela est nécessaire.

4.4. IMPACTS SUR LES SERVICES ADMINISTRATIFS

Les ministères coordonnateurs, en lien avec le SGDSN, devront déterminer, lors de la désignation de chaque opérateur d'importance vitale, si ses activités considérées comme d'importance vitale fournissent des services essentiels au sens de la directive REC. Les ministères coordonnateurs, sous couvert de la validation du SGDSN qui est l'autorité compétente identifiée auprès de la Commission européenne sur le sujet, devront également répondre aux éventuelles demandes d'organisation de mission de conseil de la Commission et

contribuer à leur préparation des missions en question. Ces missions, dont le principe devra faire l'objet d'un accord de la France, devraient demeurer marginales.

4.5. IMPACTS SOCIAUX

4.5.1. Impacts sur la société

En favorisant le partage d'informations et des bonnes pratiques au niveau européen sur les secteurs concernés par la directive REC, l'objectif est de favoriser la coordination entre Etats membres sur ces sujets, ce qui à terme devrait profiter à l'ensemble de la société européenne. En effet, les entités considérées comme critiques sont de plus en plus interdépendantes, une résilience plus importante de chaque Etat membre aura à termes des impacts sur l'ensemble des services de l'Union, en particulier sur les secteurs organisés en réseau.

4.5.2. Impact sur les personnes en situation en handicap

Sans objet.

4.5.3. Impacts sur l'égalité entre les femmes et les hommes

Sans objet.

4.5.4. Impacts sur la jeunesse

Sans objet.

4.5.5. Impacts sur les professions réglementées

Sans objet.

4.6. IMPACTS SUR LES PARTICULIERS

Sans objet.

4.7. IMPACTS ENVIRONNEMENTAUX

Sans objet.

5. CONSULTATIONS MENEES ET MODALITES D'APPLICATION

5.1. CONSULTATIONS MENEES

Une concertation de l'ensemble des ministères coordonnateurs a été réalisée sur cette mesure.

En application de l'article L. 1212-2 du code général des collectivités territoriales, les présentes dispositions ont été soumises à l'examen du Conseil national d'évaluation des normes qui a rendu un avis défavorable le 22 mai 2024.

Enfin, le service national des enquêtes administratives de sécurité, le coordinateur général de la sécurité nucléaire, le service juridique du Secrétariat général des affaires européennes et l'Agence nationale de sécurité des systèmes d'informations ont également été consultés.

5.2. MODALITES D'APPLICATION

5.2.1. Application dans le temps

Les présentes dispositions entrent en vigueur le lendemain de la publication de la présente loi au *Journal officiel* de la République française.

5.2.2. Application dans l'espace

Les présentes dispositions sont applicables de plein droit sur l'ensemble du territoire de la République conformément à l'article L. 1 du code de la défense.

Aussi, les dispositions du code de la défense créées par le présent projet de loi seront applicables de plein droit à la fois dans les collectivités régies par le principe de l'identité législative (la Guadeloupe, la Guyane, la Martinique, La Réunion, Mayotte, Saint-Barthélemy, Saint-Martin et Saint-Pierre-et-Miquelon) et par le principe de la spécialité législative (les îles Wallis et Futuna, la Polynésie française, la Nouvelle-Calédonie et les Terres australes et antarctiques françaises).

En tant que PTOM, le droit de l'union européenne ne s'applique pas à Saint-Barthélemy, Saint-Pierre-et-Miquelon, dans les îles Wallis et Futuna, en Polynésie française, Nouvelle-Calédonie et dans les Terres australes et antarctiques françaises. Les dispositions applicables aux seuls OIV exerçant des services essentiels au fonctionnement du marché intérieur de l'Union européenne ne seront donc pas applicables en l'absence d'adaptation.

5.2.3. Textes d'application

Les présentes dispositions feront l'objet d'un décret en Conseil d'Etat afin de préciser la procédure d'identification des entités critiques et l'obligation résultant de la qualification d'entité critique d'importance européenne particulière.

Article 1er (I) – Article L. 1332-10 du code de la défense

1. ETAT DES LIEUX

1.1. CADRE GENERAL

Le cadre juridique précédemment en vigueur (avant les décrets d'application de l'article 18[79] de la loi n° 2022-52 du 24 janvier 2022 relative à la responsabilité pénale et à la sécurité intérieure) résultait de l'article D. 133-10 du code de l'aviation civile qui prévoyait trois régimes encadrant la prise de vue aérienne :

- Un régime d'interdiction pour les prises de vue aérienne des zones interdites, dont la liste est fixée par un arrêté interministériel revu chaque année. La dernière version de cet arrêté a été publiée au *Journal officiel* de la République française du 13 juin 2021 (arrêté du 10 juin 2021 fixant la liste des zones interdites à la prise de vue aérienne par appareil photographique, cinématographique ou tout autre capteur de télédétection). Les dérogations sont délivrées par le ou les ministres de tutelle des zones, à l'exception des zones situées en Guyane, du ressort du préfet territorialement compétent ;
- Un régime d'autorisation pour les prises de vue aérienne en dehors du spectre visible. Les autorisations sont délivrées par le représentant de l'Etat dans le département ou le délégué du Gouvernement dans le territoire où l'utilisateur est domicilié et par le préfet de police pour les personnes résidant à Paris ;
- Un régime déclaratif pour les enregistrements d'images ou de données dans le champ du spectre visible au-dessus du territoire national (la déclaration est faite auprès du service territorial de l'aviation civile dont relève le domicile du demandeur) ;

Ces dispositions s'appliquaient sans préjudice de celles qui permettent à certains organismes et à certaines entités d'être dispensés de l'application de l'article D. 133-10 du code de l'aviation civile.

L'article 18 de la loi du 24 janvier 2022 précitée supprime les régimes d'autorisation pour la prise de vue aérienne hors du spectre visible et le régime déclaratif. Ne subsiste que le régime

[79] Décret n° 2022-1397 du 2 novembre 2022 portant application de l'article L. 6224-1 du code des transports relatif au régime encadrant la captation et le traitement des données recueillies depuis un aéronef dans certaines zones.

d'interdiction assorti de dérogations pour la captation aérienne au-dessus des zones sensibles qui, conformément à la hiérarchie des normes, est érigé au niveau législatif.

Elle étend le périmètre de l'interdiction – et par voie de conséquence des dérogations – à d'autres opérations que la seule captation d'images. En effet, elle prend en compte la transmission, la conservation, l'utilisation et surtout la diffusion des données recueillies.

Elle prévoit des sanctions pénales lorsque ces opérations ont été réalisées sans autorisation. Plus précisément, l'article L. 6232-8 du code des transports interdit le transport par aéronef sans autorisation, des explosifs, des armes, munitions de guerres. L'article interdit également le transport et l'usage des appareils photographiques au-dessus des zones interdites sans autorisation spéciale des autorités administratives. Pour cette infraction, l'article prévoit une peine d'emprisonnement d'un an et une amende de 75 000 euros d'amende. En outre, l'article L. 6232-9 du code des transports permet la confiscation et saisie des capteurs, des appareils photographiques et des clichés de zones interdites par les forces de sécurités intérieures. Enfin, l'article L. 6232-5 du code des transports prévoit l'interdiction de piloter un aéronef pour une durée pouvant aller de trois mois à trois ans.

1.2. CADRE CONSTITUTIONNEL

Il est proposé de conserver la mesure existante.

1.3. CADRE CONVENTIONNEL

Cette mesure de sécurité, existante, n'est pas immédiatement prévue par la directive REC.

1.4. ELEMENTS DE DROIT COMPARE

Sans objet.

2. NECESSITE DE LEGIFERER ET OBJECTIFS POURSUIVIS

2.1. NECESSITE DE LEGIFERER

Il est proposé de conserver cette mesure législative, sans la modifier, mais en la renumérotant pour tirer les conséquences des modifications du code de la défense par le présent projet de loi.

2.2. OBJECTIFS POURSUIVIS

Il s’agit de reprendre la disposition existante.

3. OPTIONS ENVISAGEES ET DISPOSITIF RETENU

3.1. OPTIONS ENVISAGEES

Sans objet.

3.2. DISPOSITIF RETENU

La disposition existante en matière de captation est conservée et figure désormais à l’article L. 1332-10 du code de la défense, tandis que la section I bis devient la sous-section 3. La référence aux opérateurs d’importance vitale est actualisée.

4. ANALYSE DES IMPACTS DES DISPOSITIONS ENVISAGEES

4.1. IMPACTS JURIDIQUES

4.1.1. Impact sur l’ordre juridique interne

Le présent article L. 1332-10 du code de la défense se substitue à l’actuel article L. 1332-6-1 A du code de la défense.

4.1.2. Articulation avec le droit international et le droit de l’Union européenne

Cette mesure n’est pas prévue par la directive REC.

4.2. IMPACTS ECONOMIQUES ET FINANCIERS

4.2.1. Impacts macroéconomiques

Sans objet.

4.2.2. Impacts sur les entreprises

Sans objet.

4.2.3. Impacts budgétaires

Sans objet.

4.3. IMPACTS SUR LES COLLECTIVITES TERRITORIALES

Sans objet.

4.4. IMPACTS SUR LES SERVICES ADMINISTRATIFS

Sans objet.

4.5. IMPACTS SOCIAUX

4.5.1. Impacts sur la société

Sans objet.

4.5.2. Impact sur les personnes en situation en handicap

Sans objet.

4.5.3. Impacts sur l'égalité entre les femmes et les hommes

Sans objet.

4.5.4. Impacts sur la jeunesse

Sans objet.

4.5.5. Impacts sur les professions réglementées

Sans objet.

4.6. IMPACTS SUR LES PARTICULIERS

Sans objet.

4.7. IMPACTS ENVIRONNEMENTAUX

Sans objet.

5. CONSULTATIONS MENEES ET MODALITES D'APPLICATION

5.1. CONSULTATIONS MENEES

Une concertation de l'ensemble des ministères coordonnateurs a été réalisée sur cette mesure.

En application de l'article L. 1212-2 du code général des collectivités territoriales, le présent article a été soumis à l'examen du Conseil national d'évaluation des normes qui a rendu un avis défavorable le 22 mai 2024.

Enfin, le service national des enquêtes administratives de sécurité, le coordinateur général de la sécurité nucléaire, le service juridique du Secrétariat général des affaires européennes et l'Agence nationale de sécurité des systèmes d'informations ont également été consultés.

5.2. MODALITES D'APPLICATION

5.2.1. Application dans le temps

Les présentes dispositions entrent en vigueur le lendemain de la publication de la présente loi au *Journal officiel* de la République française.

5.2.2. Application dans l'espace

Le présent article est applicable de plein droit sur l'ensemble du territoire de la République conformément à l'article L. 1 du code de la défense.

Aussi, la disposition est applicable de plein droit à la fois dans les collectivités régies par le principe de l'identité législative (la Guadeloupe, la Guyane, la Martinique, La Réunion, Mayotte, Saint-Barthélemy, Saint-Martin et Saint-Pierre-et-Miquelon) et par le principe de la spécialité législative (les îles Wallis et Futuna, la Polynésie française, la Nouvelle-Calédonie et les Terres australes et antarctiques françaises).

5.2.3. Textes d'application

Le présent article ne nécessite pas de texte d'application, se bornant à une reprise de l'existant.

Article 1er (J) – Article L. 1332-11 du code de la défense – Systèmes d'information d'importance vitale

1. ETAT DES LIEUX

1.1. CADRE GENERAL

Fin 2013, pour faire face à l'augmentation en quantité et en sophistication des attaques informatiques, 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 complété le dispositif de sécurité des activités d'importance vitale en imposant aux opérateurs d'importance vitale (OIV) le renforcement de la sécurité des systèmes d'information critiques qu'ils exploitent : les systèmes d'information d'importance vitale (SIIV).

L'Agence nationale de la sécurité des systèmes d'information (ANSSI) a pour double mission d'accompagner les opérateurs d'importance vitale (OIV) dans la sécurisation de leurs systèmes d'information critiques et de contrôler, en tant qu'autorité nationale, le respect de ce cadre réglementaire précurseur en matière de réponse à la cybermenace.

1.1.1. Les principales dispositions du dispositif SAIV (actuelle Section 2 portant sur les dispositions spécifiques à la sécurité des systèmes d'information, articles L. 1332-6-1 et suivants du code de la défense)

La déclaration des SIIV

Les OIV doivent identifier et déclarer leurs systèmes d'information d'importance vitale c'est à dire les systèmes les plus critiques pour lesquels une attaque avérée aurait des conséquences graves pour la Nation. Est entendu par système les plus critiques les systèmes sans lesquels l'opérateur ne pourrait réaliser son ou ses activités d'importance vitale ou systèmes qui concourent à la protection des sites critiques de l'opérateur. Les modalités de déclaration sont définies dans les arrêtés sectoriels.

L'obligation de notification des incidents à l'Autorité nationale de sécurité des systèmes d'information (article L. 1332-6-2 du code de la défense)

Les OIV doivent notifier directement l'autorité nationale de sécurité des systèmes d'information des incidents affectant leurs SIIV. Les types d'incidents à notifier sont spécifiques aux secteurs et précisés par arrêté.

La définition des règles de sécurité applicables aux SIIV

L'autorité nationale de sécurité des systèmes d'informations définit les règles techniques et organisationnelles de sécurité des systèmes d'information devant être appliquées par l'opérateur à ses SIIV. Elles sont au nombre de 20 et adressent les thématiques suivantes :

- Gouvernance et pilotage de la sécurité informatique,
- Maîtrise des risques,
- Maîtrise des systèmes d'information,
- Gestion des incidents de sécurité,
- Protection des systèmes d'information.

Les exigences sont définies dans des arrêtés sectoriels.

Contrôles de sécurité (article L. 1332-6-3)

L'autorité nationale de sécurité des systèmes d'information peut déclencher des contrôles de sécurité afin d'évaluer le niveau de sécurité de l'OIV. Le contrôle est conduit par l'ANSSI ou par un autre service de l'État ou par un prestataire d'audit qualifié par l'autorité nationale de sécurité des systèmes d'informations, ou le cas échéant, qualifié par l'ANSSI (PASSI LPM).

Crise majeure (article L. 1332-6-4)

Le Premier ministre peut imposer des mesures aux OIV afin de répondre à une crise majeure menaçant ou affectant la sécurité des systèmes d'information.

Ce dispositif (articles L. 1332-6-1 à L. 1332-6-6 du code de la défense) constitue une étape majeure dans le renforcement de la cybersécurité des infrastructures critiques. Il a d'ores et déjà permis de recenser les systèmes d'information les plus sensibles de la Nation, de sensibiliser les dirigeants d'OIV au risque cyber et a conduit à d'importants investissements en cybersécurité. Néanmoins, le niveau de maturité reste inégal entre les différents secteurs d'activité et de nombreux opérateurs ne disposent pas à ce jour de ressources suffisantes et de l'organisation adéquate pour piloter efficacement la sécurité de leurs systèmes d'information.

1.1.2. La directive européenne concernant les mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union (NIS 2)

Afin de garantir la résilience des « activités essentielles pour l'économie et la société de l'Union européenne », 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 (Network and Information Security, NIS) a établi les bases d'une cybersécurité renforcée pour un ensemble de secteurs d'activité sur le territoire de l'Union européenne.

Depuis 2016, la menace cyber a fortement évolué, devenant systémique. Alors que les cyber-attaquants se concentraient jusqu'à il y a quelques années sur les acteurs et opérateurs stratégiques, ils ciblent désormais l'ensemble du tissu social et économique. Au-delà de la menace stratégique (étatique) qui perdure, les cybercriminels sont rentrés dans une logique de vastes campagnes d'attaques et affectent un grand nombre de victimes (PME, collectivités territoriales, hôpitaux…), avec parfois des conséquences extrêmement dommageables pour nos concitoyens.

Face à la croissance forte de la menace cyber et l'augmentation du nombre de secteurs et organisations touchés qui en découle, la France a porté au niveau européen, pendant sa présidence du Conseil de l'Union européenne, la négociation d'une réglementation ambitieuse, la directive NIS 2[80].

Cette directive élargit considérablement le périmètre des acteurs et secteurs régulés par NIS 1. En France, cela se traduit par une augmentation du nombre d'entités régulées de 500 à 15 000 environ, et une augmentation du nombre de secteurs régulés de 6 à 18[81]. Le périmètre retenu dans le présent projet de loi cible précisément les secteurs et les types d'entités ayant le plus grand impact potentiel sur l'économie et la société françaises.

La directive élargit également le périmètre des systèmes d'information à sécuriser. Alors que NIS 1 prévoyait une identification des systèmes d'information essentiels sur lesquels les obligations de la directive porteraient, la directive NIS 2 s'applique par défaut à l'ensemble des systèmes d'information de l'entité. Des mécanismes d'exemption de certains systèmes d'information seront toutefois permis si ces derniers n'affectent pas la réalisation des activités ou la fourniture des services de l'entité.

La directive européenne NIS2 consacre elle-même le principe de proportionnalité en prévoyant deux niveaux d'entités régulées, classées selon leur degré de criticité, leur taille et leur chiffre d'affaires (pour les entreprises) : les entités essentielles et les entités importantes. Les entités essentielles sont des structures déjà sensibilisées ou confrontées à la menace cyber. Elles seront en partie des opérateurs déjà régulés, et donc déjà soumises depuis des années à la réglementation NIS et/ou au dispositif de sécurité des activités d'importance vitale (SAIV).

---

[80] 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.

[81] La directive européenne NIS 1 couvrait initialement les secteurs suivants : Eaux potables, Energie, Finances, Infrastructures Numériques, Santé, Transports. Lors de sa transposition au niveau français sont introduits les secteurs suivants : Assurance, Eaux non potables, Education, Emploi, Logistique, Restauration, Social. Dans le cadre de NIS 2, de nouveaux secteurs sont ajoutés : Services TIC (interentreprises), Administration publique (de l'Etat et du territoire), Espace, Services postaux et d'expédition, Gestion des déchets, Fabrication (dont produits chimiques), Recherche, Fournisseurs numériques, Agroalimentaire.

1.2. CADRE CONSTITUTIONNEL

Aux termes de l'article 88-1 de la Constitution : « La République participe aux Communautés européennes et à l'Union européenne, constituées d'Etats qui ont choisi librement, en vertu des traités qui les ont instituées, d'exercer en commun certaines de leurs compétences ». Le Conseil constitutionnel déduit de cette disposition que : « la transposition en droit interne d'une directive communautaire résulte d'une exigence constitutionnelle »[82]. Il en va de même pour une loi ayant pour objet d'adapter le droit interne à un règlement de l'Union européenne[83].

Les dispositions applicables aux entités critiques portent nécessairement une atteinte à la liberté d'entreprendre, laquelle découle de l'article 4 de la Déclaration des droits de l'Homme et du Citoyen de 1789[84]. Cette atteinte ne peut être ni générale ni absolue[85]. Le législateur peut limiter l'exercice de cette liberté à la condition qu'il n'en résulte pas d'atteintes disproportionnées au regard de l'objectif poursuivi[86], alors même que cette atteinte résulterait de l'exigence constitutionnelle de transposition adéquate des directives européennes[87], dans un objectif de sécurité et de défense de la Nation, en l'absence de disposition spécifique contraire de la Constitution[88] ou de mise en cause d'une règle ou d'un principe inhérent à notre identité constitutionnelle[89].

Enfin, en l'absence de remise en cause de ses garanties fondamentales, la liberté du commerce et de l'industrie ne s'oppose pas à l'intervention du législateur dans ce domaine[90].

1.3. CADRE CONVENTIONNEL

Au niveau européen, la directive (UE) 2022/2557 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience des entités critiques (REC) permet désormais d'offrir un socle minimal commun de résilience à tous les opérateurs de l'UE. Elle doit être transposée dans notre droit national d'ici le 17 octobre 2024.

---

[82] Voir notamment la décision n° 2004-496 DC du 10 juin 2004, « Loi pour la confiance dans l'économie numérique ».

[83] Voir par exemple la décision n° 2018-765, « Loi relative à la protection des données personnelles », considérant 3.

[84] Conseil constitutionnel, décision 98-401 DC du 10 juin 1998.

[85] Décision 82-141 DC du 27 juillet 1982.

[86] Décision 2023-1055 QPC du 16 juin 2023.

[87] Décision 2006-535 DC du 30 mars 2006.

[88] Décision 2004-497 DC du 1er juillet 2004.

[89] Décision 2018-765 DC du 12 juin 2018 ; décision 2019-818 QPC du 6 décembre 2019.

[90] Décision 2003-474 DC du 17 juillet 2003.

Son champ d'application couvre 11 secteurs : énergie, transports, infrastructures bancaires, infrastructures de marché financier, santé, eau potable, assainissement, infrastructures digitales, administration publique (niveau central), espace, alimentation.

De plus, il est précisé dans les deux premiers articles de la directive NIS2 que les entités désignées comme entités critiques au sens de la directive REC doivent obligatoirement être désignés par les Etats membres comme entités essentielles au sens de NIS2. Ce lien entre les deux directives est clairement explicité dans le considérant 30 de la directive NIS2 :

« Vu les liens qui existent entre la cybersécurité et la sécurité physique des entités, il convient d'assurer la cohérence des approches entre la directive (UE) 2022/2557 du Parlement européen et du Conseil et la présente directive. À cet effet, les entités recensées en tant qu'entités critiques en vertu de la directive (UE) 2022/2557 devraient être considérées comme des entités essentielles en vertu de la présente directive. De plus, chaque État membre devrait veiller à ce que sa stratégie nationale en matière de cybersécurité prévoie un cadre d'action pour une coordination renforcée en son sein entre ses autorités compétentes en vertu de la présente directive et les autorités compétentes en vertu de la directive (UE) 2022/2557, dans le contexte du partage d'informations relatives aux risques et aux menaces et incidents en matière de cybersécurité, ainsi qu'aux risques et aux menaces et incidents non liés à la cybersécurité, et de l'exercice des tâches de supervision. Les autorités compétentes en vertu de la présente directive et les autorités compétentes en vertu de la directive (UE) 2022/2557 devraient coopérer et échanger des informations sans retard injustifié, notamment en ce qui concerne le recensement des entités critiques, les risques, les menaces et incidents en matière de cybersécurité, ainsi que les risques, menaces et incidents non liés à la cybersécurité affectant les entités critiques, y compris les mesures physiques et de cybersécurité adoptées par les entités critiques ainsi que les résultats des activités de supervision réalisées à l'égard de ces entités ».

L'alinéa 3 de l'article 2 de la directive NIS2 prévoit que les entités critiques désignées au titre de la directive REC entrent dans le champ d'application de la directive NIS2 et doivent être considérées comme des entités essentielles au titre de cette même directive (article 1, alinéa 1, paragraphe f).

1.4. ELEMENTS DE DROIT COMPARE

Sans objet.

2. NECESSITE DE LEGIFERER ET OBJECTIFS POURSUIVIS

2.1. NECESSITE DE LEGIFERER

La nécessité de légiférer est requise par la transposition de la directive européenne (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 (NIS 2), notamment ses deux premiers articles. Les besoins de coordination entre les autorités compétentes des directives REC et NIS2 est également rappelé dans les considérants 9 ; 13 ; 20 ; 24 ; 40 de la directive sur la résilience des entités critiques (REC) du 14 décembre 2022. La coordination entre les autorités compétentes de ces deux directives est également demandée dans les articles 1 ; 4 ; 6 ; 9 et 21 de la directive REC.

La prise en compte des dispositions de ces deux directives implique un changement du droit national : les obligations cyber actuelles des opérateurs d'importance vitale ne portaient que sur les Systèmes d'informations d'importance vitale (SIIV), donc certains systèmes d'informations de l'opérateur, ceux identifiés par lui comme les plus sensibles. La directive NIS2 va plus loin dans la logique de résilience, étant donné que tous les systèmes d'informations des opérateurs identifiés comme critiques au titre de la directive REC devront appliquer les obligations de NIS2 en tant qu'entités essentielles.

2.2. OBJECTIFS POURSUIVIS

Le dispositif actuel de SAIV prend déjà en compte les SIIV. L'objectif du présent projet de loi est double : conservation des dispositions existantes et transpositions des 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 (NIS 2). ainsi que la directive (UE) 2022/2557 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience des entités critiques (REC). Les deux textes font en effet référence dans plusieurs de leurs articles évoqués infra à l'autre directive.

3. OPTIONS ENVISAGEES ET DISPOSITIF RETENU

3.1. OPTIONS ENVISAGEES

Sans objet.

3.2. DISPOSITIF RETENU

La nouvelle sous-section 4 « Dispositions applicables aux systèmes d'information » reprend les dispositions qui figuraient dans la section 2 « Dispositions spécifiques à la sécurité des systèmes d'information » du code de la défense (articles L. 1332-6-1 à L. 1332-6-6), qui imposait des mesures de protection cyber aux OIV.

Le présent article impose également à tous les OIV de mettre en œuvre les obligations prévues au titre du Chapitre II du présent projet de loi « De la cyber résilience », à savoir :

- Article 14 : mise en œuvre de mesures de résilience cyber (instauration d'une gouvernance de sécurité des réseaux et SI, de formation à la cybersécurité, destinées à assurer la protection des réseaux et SI y compris en cas de sous-traitance, mise en place d'outils et de procédures pour assurer la défense des réseaux et SI et de gérer les incidents, garantir la résilience des activités) ;
- Article 16 : identification par les opérateurs de leur SIIV ;
- Article 17 : notification obligatoire des incidents cyber.

4. ANALYSE DES IMPACTS DES DISPOSITIONS ENVISAGEES

4.1. IMPACTS JURIDIQUES

4.1.1. Impacts sur l'ordre juridique interne

Le présent article L. 1332-11 (sous-section 4 « Dispositions applicables aux systèmes d'information ») remplace la section 2 « Dispositions spécifiques à la sécurité des systèmes d'information » du code de la défense (articles L. 1332-6-1 à L. 1332-6-6)

4.1.2. Articulation avec le droit international et le droit de l'Union européenne

Les dispositions de la présente mesure s'inscrivent dans le champ de la transposition de la directive européenne sur la résilience des entités critiques du (REC) du 14 décembre 2022, notamment ses articles 1, 4, 6, 9 et 21.

4.2. IMPACTS ECONOMIQUES ET FINANCIERS

4.2.1. Impacts macroéconomiques

Sans objet.

4.2.2. Impacts sur les entreprises

Se référer aux éléments fournis *infra* pour les articles 14 et 16 du projet de loi, au sein la section prévue pour la transposition de la directive européenne (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 (NIS 2).

4.2.3. Impacts budgétaires

Se référer aux éléments fournis *infra* pour les articles 14 et 16 du projet de loi, au sein la section prévue pour la transposition de la directive européenne (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 (NIS 2).

4.3. IMPACTS SUR LES COLLECTIVITES TERRITORIALES

Se référer aux éléments fournis *infra* pour les articles 14 et 16 du projet de loi, au sein la section prévue pour la transposition de la directive européenne (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 (NIS 2).

4.4. IMPACTS SUR LES SERVICES ADMINISTRATIFS

Se référer aux éléments fournis *infra* pour les articles 14 et 16 du projet de loi, au sein la section prévue pour la transposition de la directive européenne (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 (NIS 2).

4.5. IMPACTS SOCIAUX

4.5.1. Impacts sur la société

Le renforcement des exigences en matière de sécurité des systèmes d'information d'importance vitale doit permettre de limiter les impacts d'une crise ou de problèmes majeurs d'un opérateur d'importance vitale sur le fonctionnement de la société.

4.5.2. Impact sur les personnes en situation en handicap

Sans objet.

4.5.3. Impacts sur l'égalité entre les femmes et les hommes

Sans objet.

4.5.4. Impacts sur la jeunesse

Sans objet.

4.5.5. Impacts sur les professions réglementées

Sans objet.

4.6. IMPACTS SUR LES PARTICULIERS

Sans objet.

4.7. IMPACTS ENVIRONNEMENTAUX

Sans objet.

5. CONSULTATIONS MENEES ET MODALITES D'APPLICATION

5.1. CONSULTATIONS MENEES

Une concertation a été réalisée avec l'ensemble des ministères coordonnateurs et l'Agence Nationale de la Sécurité des Systèmes d'information (ANSSI).

En application de l'article L. 1212-2 du code général des collectivités territoriales, le présent article a été soumis à l'examen du Conseil national d'évaluation des normes qui a rendu un avis défavorable le 22 mai 2024.

Enfin, le service national des enquêtes administratives de sécurité, le coordinateur général de la sécurité nucléaire, le service juridique du Secrétariat général des affaires européennes et l'Agence nationale de sécurité des systèmes d'informations ont également été consultés.

5.2. MODALITES D'APPLICATION

5.2.1. Application dans le temps

Les présentes dispositions entrent en vigueur le lendemain de la publication de la présente loi au *Journal officiel* de la République française.

Les opérateurs d'importance vitale désignés avant l'entrée en vigueur des dispositions du titre I^{er} de la présente loi doivent être regardés comme désignés en application du I de l'article L. 1332-2 du code de la défense dans sa rédaction résultant du chapitre I^{er} de la loi à la date de son entrée en vigueur.

Ces opérateurs restent soumis aux obligations qui leurs sont applicables avant l'entrée en vigueur de la présente loi jusqu'à l'accomplissement des obligations prévues aux articles L. 1332-2 à L. 1332-5 et à l'article L. 1332-11 dans leur rédaction résultant de la présente loi.

5.2.2. Application dans l'espace

Le présent article est applicable de plein droit sur l'ensemble du territoire de la République conformément à l'article L. 1 du code de la défense.

Aussi, les dispositions du code de la défense créées par le présent projet de loi seront applicables de plein droit à la fois dans les collectivités régies par le principe de l'identité législative (la Guadeloupe, la Guyane, la Martinique, La Réunion, Mayotte, Saint-Barthélemy, Saint-Martin et Saint-Pierre-et-Miquelon) et par le principe de la spécialité législative (les îles Wallis et Futuna, la Polynésie française, la Nouvelle-Calédonie et les Terres australes et antarctiques françaises).

Le présent article renvoie à l'article L. 1332-2 du code de la défense, qui renvoie lui-même à des dispositions du code de l'environnement qui ne sont pas applicables à Saint-Barthélemy, dans les îles Wallis et Futuna, en Polynésie française, en Nouvelle-Calédonie et dans les Terres australes et antarctiques françaises, les collectivités étant compétentes dans cette matière. Si l'article L. 6311-1 du code de la défense prévoit déjà une grille de lecture générale qui couvre toute la partie législative pour son application dans les îles Wallis et Futuna, en Polynésie française, en Nouvelle-Calédonie et dans les Terres australes et antarctiques françaises, il n'existe de grille similaire pour Saint-Barthélemy. Il est proposé de créer une grille sur le même modèle au sein d'un nouvel article L. 6221-2 du code de la défense, par l'article 3 du présent projet de loi.

Par ailleurs, en tant que PTOM, le droit de l'union européenne ne s'applique pas à Saint-Barthélemy, Saint-Pierre-et-Miquelon, dans les îles Wallis et Futuna, en Polynésie française, Nouvelle-Calédonie et dans les Terres australes et antarctiques françaises. Les dispositions applicables aux seuls OIV exerçant des services essentiels au fonctionnement du marché intérieur de l'Union européenne ne seront donc pas applicables en l'absence d'adaptation.

5.2.3. Textes d'application

Le présent article fera l'objet d'un décret en Conseil d'Etat résultant de la transposition de la directive NIS 2 distinct de celui portant sur l'application du titre I^{er} du projet de loi. Ce décret en Conseil d'Etat ne sera pas codifié dans le code de la défense.

Article 1er (K) – Articles L. 1332-12 à L. 1332-14 du code de la défense – Habilitation et contrôles

1. ETAT DES LIEUX

1.1. CADRE GENERAL

Il existe d'ores et déjà des procédures de contrôle des obligations applicables aux opérateurs d'importance vitale. Elles se déclinent selon les secteurs d'activités.

Pour le secteur des activités militaires de l'Etat, les procédures de contrôle sont définies dans les DNS « activités militaires de l'Etat » et « activités industrielles de l'armement » ainsi que par les dispositions contenues au chapitre 5 de l'instruction générale interministérielle (IGI) 6600 du 7 janvier 2014 relative la sécurité des activités d'importance vitale[91]. Les autorités de contrôle sont en effet différentes pour ces secteurs d'activités spécifiques afin de correspondre au mieux aux spécificités des secteurs ainsi qu'à l'organisation des forces armées sur le territoire national.

Pour le sous-secteur d'activité du nucléaire, elles sont définies par la DNS « nucléaire » ainsi que par les dispositions contenues au chapitre 6 de l'IGI 6600 du 7 janvier 2014 précitée. Ce suivi particulier a deux objectifs : en premier lieu, faire en sorte que les obligations de la SAIV soient en adéquation avec les obligations nationales et internationales des installations nucléaires, très normées (suivi par l'Agence Internationale de l'Energie Atomique, application des obligations des articles L. 1333-1 et suivants du code de la défense), mais également prendre en compte la spécificité de ce secteur pour la SAIV. En effet, un grand nombre d'opérateurs désignés au titre de la DNS « nucléaire » le sont au titre du danger grave qu'ils pourraient porter à la population (actuel L. 1332-2 du code de la défense) et doivent donc faire l'objet d'un traitement particulier.

Si le suivi des « activités militaires de l'Etat », « activités industrielles de l'armement » ou « nucléaire » fait l'objet d'un traitement particulier, le suivi des autres secteurs s'articule comme suit.

Les préfets de département approuvent les PPP et élaborent les PPE. Ils ont également, conformément à l'article R. 1332-29 du code de la défense, la responsabilité de s'assurer régulièrement du bon niveau de protection des PIV, par un dialogue permanent entre les préfectures et les délégués pour la défense et la sécurité locaux identifiés pour chaque point d'importance vitale par l'opérateur. Cette responsabilité comprend la possibilité de visite sur

[91] https://www.legifrance.gouv.fr/circulaire/id/37828.

site du PIV concerné. Dans ce cas, le préfet de département ou son représentant peut être accompagné d'experts des services déconcentrés de l'Etat en fonction de la nature du PIV. L'article R. 1332-30 du code de la défense précise ce pouvoir des préfets de départements – ou de l'autorité désignée par le ministre de la défense pour les opérateurs suivis par ce dernier -, car il permet aux autorités compétentes de mettre l'opérateur en demeure d'exécuter cette mesure *« dans un délai compris entre un mois et trois mois selon la nature de la mesure »* dans le cas où l'opérateur n'a pas réalisé une mesure de protection prévue dans son plan particulier de protection. Dans le cas où, après l'expiration du délai l'autorité constate que la mesure n'a pas été mise en œuvre, celle-ci peut saisir *« l'autorité judiciaire aux fins de poursuite de l'auteur du délit prévu par les dispositions du premier alinéa de l'article L. 1332-7 »*, article qui fixe les dispositions pénales que peut encourir un opérateur d'importance vitale en cas de manquement à ses obligations.

Par ailleurs, le préfet de département dispose de la possibilité de solliciter le contrôle d'un PIV par la Commission zonale de défense et de sécurité (CZDS) (article R. 1332-15 du code de la défense). Afin de permettre à la CZDS d'effectuer une programmation des contrôles de PIV, les préfets de département la tiennent régulièrement informée de l'approbation des PPP.

La Commission interministérielle de défense et de sécurité et la Commission zonale de défense et de sécurité sont chargées d'une mission générale de contrôle de la mise en œuvre du dispositif de protection des PIV et zones d'importance vitale, c'est-à-dire les zones qui englobent plusieurs points d'importance vitale, à l'exception de ceux dépendant d'OIV relevant du ministre de la défense. Elles peuvent, à leur initiative ou sur demande d'un ministre coordonnateur ou d'un préfet de département, contrôler les mesures prises pour la sécurité des PIV ou des ZIV. La CZDS ne contrôle que les points et les zones d'importance vitale situés dans sa zone de compétence, et donc sa zone de défense et de sécurité.

La CIDS peut émettre des directives d'inspection. A cet égard, elle peut fixer annuellement, sur proposition du SGDSN (et de l'ANSSI), la liste des PIV qui en raison de la criticité potentielle de leur système d'information doivent faire l'objet d'un contrôle. Des représentants de l'ANSSI font alors partie des équipes chargées du contrôle de ces PIV et réalisent le contrôle du système d'information ainsi que du site. L'ANSSI peut également, à sa demande, se joindre aux équipes chargées des contrôles des autres PIV.

Afin de coordonner les prévisions de contrôle, en prenant en compte les éventuelles directives d'inspection émises par la CIDS, les CZDS transmettent au SGDSN ainsi qu'au ministère de l'intérieur, au titre de l'animation territoriale :

- un calendrier annuel prévisionnel de contrôles ;
- un bilan annuel des contrôles effectués au titre de l'année passée.

Dans la perspective d'un contrôle, la CZDS demandera en tant que de besoin communication du PPP approuvé au préfet de département.

Les dispositions ci-après donnent des indications sur le déroulement du contrôle, sans préjuger des adaptations nécessaires au cas par cas, laissées à l'appréciation de la CZDS.

Objectifs du contrôle

Le nombre total de PIV ne permet pas aux seules commissions de contrôler l'intégralité des PIV relevant de leur ressort territorial. Les contrôles de la commission sont ainsi complémentaires avec la mission générale de vérification de la réalisation des PPP dévolue aux préfets de département, qui sont associés à la politique de contrôle.

Après un contrôle ayant donné lieu à des recommandations à l'opérateur, la vérification de la mise en œuvre de ces recommandations incombe à l'autorité de contrôle, qui en informera le préfet de département.

Si les documents de référence concernant la sécurité du PIV sont d'abord la DNS, le PSO et le PPP, la commission peut vérifier, plus généralement, que les mesures de sécurité ne contiennent pas de failles évidentes en matière de protection des installations contre la malveillance.

Préparation du contrôle sur place

Dans l'esprit de coopération avec les opérateurs qui sous-tend la démarche SAIV, les contrôles sont annoncés, et non impromptus. Le président de la commission informe par écrit le délégué pour la défense et la sécurité du PIV de la date et de l'objet du contrôle ou de la visite sur site, de la composition de l'équipe de contrôle et du programme prévisionnel et, si possible, de l'horaire. Il signale le cas échéant les points particuliers sur lesquels portera le contrôle. Lorsque le contrôle est mené par une commission, le préfet de département en est informé et peut formuler un avis quant à son opportunité.

En cas de contrôle d'une ZIV, le délégué pour la défense et la sécurité de la ZIV est le correspondant de l'équipe de contrôle.

Le contrôle se déroule idéalement sur une seule journée. Lorsqu'il porte aussi sur la sécurité des systèmes d'information, le contrôle peut nécessiter normalement trois à quatre journées supplémentaires mais ne mobilise que les experts de la sécurité des systèmes d'information de l'équipe de contrôle (les représentants de l'ANSSI) et du PIV. Le contrôle peut être prolongé si l'étendue ou la complexité du PIV le justifie, sur décision du président de la commission ou du préfet de département en tant qu'autorité de contrôle.

Le contrôle des PIV est effectué par des membres de la CZDS ou leurs représentants, préalablement formés à la sécurité des activités d'importance vitale, accompagnés en tant que de besoin par des experts en fonction de la nature du PIV. Ils forment une équipe de contrôle. Tous les membres de l'équipe de contrôle doivent posséder une habilitation de niveau secret défense.

La composition de l'équipe de contrôle est adaptée en fonction des enjeux de sécurité du PIV, de la durée du contrôle (sur un ou plusieurs jours) et des expertises particulières recherchées. Néanmoins, c'est au président de la commission ou à son représentant qu'il appartient de définir le format de cette équipe. Le chef de la délégation est le président de la commission ou son représentant. Les domaines d'expertise requis pour le contrôle sont notamment la gestion de risques, la sûreté, la sécurité physique des installations et la sécurité des systèmes d'information.

A ce titre, l'équipe de contrôle de la CZDS est typiquement composée de la manière suivante :

- un représentant du préfet de zone de défense et de sécurité, chef de la délégation et chargé de produire le rapport ;
- un représentant du préfet de département ayant approuvé le PPP, s'il le souhaite ;
- un représentant du service de gendarmerie ou de police territorialement compétent ;
- un représentant du ministère coordonnateur, au titre de son expertise ;
- des experts de l'Agence nationale de la sécurité des systèmes d'information notamment lorsqu'il s'agit d'un contrôle demandé par l'ANSSI.

Une réunion préparatoire au contrôle est organisée avec les participants sélectionnés, le ministère coordonnateur concerné ou son représentant déconcentré et toute autre personne dont la présence lui paraît justifiée. La participation du DDS du PIV concernée est indispensable.

Les objectifs de cette réunion sont de :

- procéder à un examen rapide des caractéristiques du PIV contrôlé, sur la base des documents existants (PPP, PPE, PSO, DNS, rapport de contrôle antérieur) ;
- définir les axes principaux du contrôle sur site et les points saillants à vérifier, régler les aspects logistiques notamment les moyens d'accès aux composants névralgiques, les moyens de contrôle (droits d'accès, outils, etc.), les modalités pratiques du déplacement.

Le chef de délégation effectue la répartition des tâches entre les membres de l'équipe de contrôle.

L'équipe de contrôle doit prendre connaissance du référentiel de sécurité du site constitué par le PPP et le PSO. L'économie générale de la gestion de la sûreté du PIV, l'analyse de risque sur laquelle elle repose et l'organisation de la défense en profondeur du site doivent être assimilées et les composants névralgiques du PIV identifiés.

Le représentant de la préfecture de département, s'il est présent, fait connaître ce qu'il sait du PIV. Notamment, il fait savoir à l'équipe de contrôle l'état d'avancement de la mise en œuvre

du PPP et si certaines des mesures de protection prévues dans celui-ci ne sont pas encore mises en place.

Des éléments de contexte et informations complémentaires à celles contenues dans le PPP sont apportés, comme :

- l'environnement du site (zone urbaine ou rurale, isolement, etc.) ;
- les autres réglementations de sécurité ou sûreté auxquelles il est éventuellement soumis (ISPS, OACI, ZRR, ICPE, Seveso, INB, zone d'interdiction de survol ou de prise de vues aériennes, zones protégées, etc.) ;
- d'une manière générale, toutes données intéressantes au titre de la sécurité du site (sensibilité ou vulnérabilité particulière, incidents de sécurité répertoriés, etc.).

Déroulement du contrôle

Le contrôle doit être exécuté de sorte à pouvoir déterminer si le dispositif de défense en profondeur du PIV est cohérent avec le PPP et les exigences minimales de sûreté attendues sur le site. De même l'adéquation avec le PPE peut être vérifiée.

a - Confidentialité du déroulement du contrôle

Les membres de l'équipe de contrôle font preuve sur place de discrétion vis-à-vis du personnel et des autres visiteurs présents sur le PIV. Les réunions se tiennent dans une salle dédiée au sein du PIV afin d'assurer la confidentialité des entretiens. Tous les participants doivent être habilités au secret de la défense nationale

b - Etapes du contrôle

Les étapes prévues ci-après sont indicatives et s'adaptent à chaque cas.

- Etape 1 : réunion de lancement du contrôle

Le chef de délégation introduit la séance de lancement du contrôle en présentant un bref rappel des tenants et aboutissants du dispositif de la SAIV, du rôle des acteurs, de l'objectif du contrôle et de la composition de l'équipe de contrôle.

Le caractère classifié des informations échangées et des documents étudiés est rappelé. La présence des personnels du PIV participant au contrôle est nécessaire pour assurer que l'ensemble des intervenants de l'opérateur comprend le cadre général dans lequel s'inscrit le contrôle.

- Etape 2 : présentation sur table du PIV et du PPP par l'opérateur

L'opérateur présente le PIV et le PPP pour permettre à l'équipe de contrôle d'apprécier sur table la politique générale de sécurité du PIV. Il précise l'activité du PIV, son organisation, son fonctionnement et les grandes lignes de l'analyse de risque du PPP (scénarios de menace, vulnérabilités).

- Etape 3 : contrôle des mesures de protection

- Protection physique

Le site est visité avec l'opérateur selon une logique concentrique, de l'extérieur (contour et entrée du PIV) vers l'intérieur (composants névralgiques du PIV). Le système de défense en profondeur doit ainsi pouvoir être identifié et compris, ses éventuelles lacunes détectées.

Les mesures de sécurité existantes sont comparées aux prescriptions du PPP et leur pertinence est jugée non seulement par rapport à l'analyse de risque qu'il contient mais aussi par rapport aux vulnérabilités identifiées par ailleurs par l'équipe de contrôle.

Le contrôle des mesures du plan VIGIPIRATE applicables au PIV est effectué. Sont notamment vérifiées l'application des mesures actives et la préparation des autres mesures graduées prévues dans le PPP comme par exemple le contrôle des personnes ou les mesures face aux menaces NRBC-E.

- Sécurité des systèmes d'information

Le contrôle de la sécurité des systèmes d'information est effectué lorsqu'un système d'information constitue ou est susceptible de constituer un composant névralgique du PIV (pouvant alors être désigné comme système d'information d'importance vitale, comme défini à l'actuel L. 1332-6-1).

Le contrôle comporte une analyse technique du niveau de sécurité du système d'information, au regard des mesures de sécurité des systèmes d'information présentées dans le PPP, mais aussi par rapport aux menaces et vulnérabilités identifiées par ailleurs par l'équipe de contrôle, sur site, et à la lecture des documents transmis.

Les contrôles ne se limitent donc pas à un audit de l'organisation SSI (procédures, maintien en condition de sécurité) et à un contrôle de la sécurité physique des composants du système d'information, mais incluent également un examen technique du système d'information pouvant notamment comprendre :

- le relevé d'informations techniques (configurations du système, journaux d'évènements, traces d'incidents, etc.) ;
- la réalisation de tests d'intrusion dans le système d'information ;
- l'analyse du code source des logiciels ;
- la conduite d'entretiens avec les personnes en charge de l'administration du système ;

– et plus généralement toutes actions permettant d'analyser le niveau de sécurité.

Les interventions réalisées sont conformes à celles définies lors de la planification du contrôle. Une convention entre l'OIV et l'ANSSI peut être préalablement établie en tant que de besoin pour préciser les conditions dans lesquelles ces interventions sont effectuées. Sous son contrôle, le PIV met à disposition de l'ANSSI un accès direct à son système d'information pour permettre ces interventions.

- Dispositif de gestion de crise et plan de continuité d'activité

L'organisation mise en place pour traiter les crises et assurer la continuité et le rétablissement d'activités du site font partie des éléments contrôlés. A ce titre, les membres de la commission de contrôle peuvent exiger d'avoir accès au plan de continuité d'activité de l'OIV, éventuellement décliné localement.

- Etape 4 : bilan avec l'opérateur

Un bilan immédiat est effectué à la fin du contrôle en présence du délégué à la défense et à la sécurité ainsi que du responsable de la sécurité des systèmes d'information de l'opérateur. Cette réunion de clôture a pour objectif de présenter à l'opérateur l'appréciation de l'équipe de contrôle sur la sécurité du PIV et de recueillir son avis en vue de tirer les conclusions initiales essentielles.

Les points suivants sont notamment abordés :

– conformité des mesures de sécurité avec le contenu du PPP ;
– pertinences des mesures de sécurité mises en place ;
– principales failles de sécurité détectées au regard des risques identifiés ;
– application des mesures VIGIPIRATE ;
– principaux axes d'amélioration.

La nature des principales non-conformités des mesures de protection avec le PPP est constatée avec le DDS. Les failles importantes dans l'analyse de risque, identifiées pendant le contrôle, mais non traitées par le PPP, sont aussi constatées.

Rapport de contrôle

Enfin, un rapport de contrôle est établi.

L'objectif du rapport de contrôle est de présenter à l'opérateur des recommandations pour améliorer la protection du PIV par rapport à son contexte, à l'état de l'art, et à son référentiel de sécurité (PPP, PSO, DNS). Il met donc en évidence les vulnérabilités du PIV face aux menaces identifiées et les mesures à prendre pour réduire la probabilité d'occurrence et/ou l'impact des risques. Parmi ces mesures, on distingue :

- les recommandations simples pour les problèmes les moins graves, qui ne donneront pas lieu à des suites particulières ;
- les préconisations, appelant une action de l'opérateur et/ou la révision du PPP.

Le rapport de contrôle est classifié et respecte un plan type.

Il commence par une brève description des modalités du contrôle, puis une page de synthèse sur le niveau de protection du PIV constaté pendant le contrôle, les principales failles détectées dans la sûreté du PIV, les recommandations et préconisations faites à l'opérateur.

Le rapport est rédigé par le chef de la délégation, approuvé par la commission et validé par son président. Il est ensuite transmis au DDS qui peut formuler des observations écrites, lesquelles pourront être annexées au rapport ou mener à sa révision.

Le rapport est soumis par le chef de délégation à l'autorité en charge du contrôle (CIDS, CZDS ou préfet de département) avant son adoption définitive.

Le rapport est adressé au :

- DDS du PIV ;
- DDS de l'OIV ;
- aux préfets de zone de défense et de sécurité et de département concernés ;
- au(x) ministre(s) coordonnateur(s) concernés ;
- au SHFD du ministère de l'intérieur, au titre de l'animation territoriale ;
- au SGDSN.

Le suivi des préconisations figurant dans le rapport du contrôle incombe à l'autorité de contrôle. Lorsque les préconisations concernent la sécurité des systèmes d'information, l'autorité de contrôle peut faire appel aux personnes qualifiées ayant participé au contrôle (i.e. les experts de l'ANSSI) pour s'assurer du suivi de ces préconisations.

L'autorité de contrôle est informée des suites données à son rapport, tout comme le préfet de département.

De manière générale, le contrôle du PIV peut conduire à :

- la révision du PPP (Art. R. 1332-31 du code de la défense) ;
- la mise en demeure de l'OIV d'exécuter, dans un délai compris entre un et trois mois, une ou plusieurs mesures du PPP qui n'auraient pas été réalisées (Art. R. 1332-30 du code la défense);
- la saisine de l'autorité judiciaire aux fins de poursuite de l'auteur du délit (Art. R. 1332-30 du code de la défense).

1.2. CADRE CONSTITUTIONNEL

Aux termes de l'article 88-1 de la Constitution : « La République participe aux Communautés européennes et à l'Union européenne, constituées d'Etats qui ont choisi librement, en vertu des traités qui les ont instituées, d'exercer en commun certaines de leurs compétences ». Le Conseil constitutionnel déduit de cette disposition que : « la transposition en droit interne d'une directive communautaire résulte d'une exigence constitutionnelle »[92]. Il en va de même pour une loi ayant pour objet d'adapter le droit interne à un règlement de l'Union européenne[93].

Les dispositions applicables aux entités critiques portent nécessairement une atteinte à la liberté d'entreprendre, laquelle découle de l'article 4 de la Déclaration des droits de l'Homme et du Citoyen de 1789[94]. Cette atteinte ne peut être ni générale ni absolue[95]. Le législateur peut limiter l'exercice de cette liberté à la condition qu'il n'en résulte pas d'atteintes disproportionnées au regard de l'objectif poursuivi[96], alors même que cette atteinte résulterait de l'exigence constitutionnelle de transposition adéquate des directives européennes[97], dans un objectif de sécurité et de défense de la Nation, en l'absence de disposition spécifique contraire de la Constitution[98] ou de mise en cause d'une règle ou d'un principe inhérent à notre identité constitutionnelle[99].

Enfin, en l'absence de remise en cause de ses garanties fondamentales, la liberté du commerce et de l'industrie ne s'oppose pas à l'intervention du législateur dans ce domaine[100].

En l'espèce, l'exigence d'une transposition complète de la directive REC, qui impose de prévoir un mécanisme de supervision, doit s'accompagner de garanties offertes aux opérateurs concernés dans la conduite des contrôles. L'assermentation des agents de contrôle permet de confier à ces agents une possibilité de rédiger des procès-verbaux qui font foi jusqu'à preuve du contraire.

Ces garanties sont indispensables pour s'assurer d'une procédure répondant à l'ensemble des exigences qui s'imposent dans le cas où une sanction administrative peut être infligée à un

---

[92] Voir notamment la décision n° 2004-496 DC du 10 juin 2004, « Loi pour la confiance dans l'économie numérique ».

[93] Voir par exemple la décision n° 2018-765, « Loi relative à la protection des données personnelles », considérant 3.

[94] Conseil constitutionnel, décision 98-401 DC du 10 juin 1998.

[95] Décision 82-141 DC du 27 juillet 1982.

[96] Décision 2023-1055 QPC du 16 juin 2023.

[97] Décision 2006-535 DC du 30 mars 2006.

[98] Décision 2004-497 DC du 1er juillet 2004.

[99] Décision 2018-765 DC du 12 juin 2018 ; décision 2019-818 QPC du 6 décembre 2019.

[100] Décision 2003-474 DC du 17 juillet 2003.

opérateur privé, ce qui a nécessairement des effets sur ses libertés économiques dans les limites détaillées précédemment.

1.3. CADRE CONVENTIONNEL

Au niveau européen, la directive (UE) 2022/2557 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience des entités critiques (REC) permet désormais d'offrir un socle minimal commun de résilience à tous les opérateurs de l'UE. Elle doit être transposée dans notre droit national d'ici le 17 octobre 2024.

Son champ d'application couvre 11 secteurs : énergie, transports, infrastructures bancaires, infrastructures de marché financier, santé, eau potable, assainissement, infrastructures digitales, administration publique (niveau central), espace, alimentation.

L'article 21 de la directive REC prévoit que : « Afin d'évaluer le respect des obligations découlant de la présente directive par les entités qu'ils ont recensées en tant qu'entités critiques en vertu de l'article 6, paragraphe 1, de la présente directive, les États membres veillent à ce que les autorités compétentes disposent des pouvoirs et des moyens nécessaires pour: a) procéder à des inspections sur place de l'infrastructure critique et des locaux utilisés par l'entité critique pour fournir ses services essentiels et à la supervision à distance des mesures prises par les entités critiques conformément à l'article 13; b) effectuer ou ordonner des audits portant sur ces entités critiques ».

De plus, l'article 22 de la directive REC 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. Ces sanctions doivent être effectives, proportionnées et dissuasives. Les États membres informent la Commission, au plus tard le 17 octobre 2024 du régime ainsi déterminé et des mesures ainsi prises, de même que, sans retard, de toute modification apportée ultérieurement à ce régime ou à ces mesures. »

1.4. ELEMENTS DE DROIT COMPARE

Sans objet.

2. NECESSITE DE LEGIFERER ET OBJECTIFS POURSUIVIS

2.1. NECESSITE DE LEGIFERER

L'article 34 de la Constitution dispose que « la loi fixe les règles concernant […] la procédure pénale » ainsi que « l'assiette, le taux et les modalités de recouvrement des impositions de toutes natures ».

Dans la mesure où les dispositions envisagées sont relatives à la procédure de recherche et de constatation d'infractions par les opérateurs d'importance vitale, en vertu des obligations qui sont les leurs en cette qualité, par des agents assermentés mais ne disposant pas du statut d'officier de police judiciaire, toute modification de cette matière relève du domaine législatif.

De surcroît, les recherches menées par ces agents assermentés font l'objet d'un compte-rendu, qui doit être transmis *« sans délai au Procureur de la République »*, en cas de constatations effectives d'une ou plusieurs infractions.

La nécessité de légiférer est également liée aux articles 21 et 22 de la directive REC, qui établissent que les autorités compétentes des Etats membres disposent « des pouvoirs et moyens nécessaires » pour assurer le suivi de leurs entités critiques. Ce suivi intègre des inspections sur pièces et sur place ainsi que des audits. De telles dispositions de contrôles accordés aux pouvoirs publics sur des entités publiques comme privées doivent être inscrites dans le cadre législatif.

2.2. OBJECTIFS POURSUIVIS

L'objectif principal des présentes dispositions est d'assurer la qualité et l'impartialité de l'instruction des dossiers de saisine de la Commission des sanctions mentionnée à l'article L. 1332-15 du présent projet de loi, notamment grâce aux données et constatations collectées et aux rapports formulés à l'occasion des contrôles des OIV. L'objectif est également de donner un certain nombre de garanties aux opérateurs mais également de sanctionner spécifiquement, comme en matière fiscale, tout comportement qui aurait pour effet de faire obstacle à la conduite du contrôle.

Il s'agit enfin de mettre en cohérence notre dispositif actuel avec les obligations et l'esprit de la directive REC, en encadrant le statut et les missions des agents chargés de la supervision des opérateurs. Cet objectif implique de pouvoir :

- Ancrer le rôle des chargés de mission de sécurité économique présents en zone de défense et de sécurité, qui sont les agents chargés de suivre le dispositif SAIV et donc d'animer la politique publique sur le territoire. Ces agents effectuent déjà des contrôles chez les opérateurs, et l'enjeu est donc d'entériner le rôle qu'ils effectuent actuellement au sein du dispositif SAIV ;
- Eclaircir la marge de manœuvre des préfectures de départements (ou de l'autorité désignée par le ministre de la défense pour les activités relevant de son ministère) dans les contrôles qu'elles peuvent effectuer chez les opérateurs. En effet, s'il est prévu

dans la législation et la réglementation que les préfectures sont compétentes pour valider les plans particuliers de protection et s'assurer de leur bonne mise en œuvre, il n'est pas précisé – que ce soit au niveau réglementaire ou dans l'IGI 6600 – les modalités de contrôles ou de visites des préfectures sur site ;

- Créer des possibilités pour les ministères coordonnateurs de faire constater des manquements de leurs opérateurs, en particulier pour la réalisation des plans de sécurité opérateur. En effet, si aujourd'hui les autorités en charge de l'approbation des plans particuliers de protection ont la possibilité de prendre des arrêtés de mise en demeure à l'encontre des opérateurs, ce n'est pas le cas pour les ministères coordonnateurs. Ces derniers doivent pourtant vérifier et valider que les plans de sécurité opérateur sont réalisés dans les temporalités fixées par voie réglementaire, et que les objectifs desdits plans correspondent aux scénarios de risques et de menaces fixés dans les directives nationales de sécurité ;
- Assurer un parallélisme et une synergie avec le dispositif retenu pour les constations des manquements cyber, qui sont effectués par des agents assermentés de l'autorité nationale de sécurité des systèmes d'information ou des organismes indépendants qu'elle désigne – cf. article 26 du présent projet de loi.

3. OPTIONS ENVISAGEES ET DISPOSITIF RETENU

3.1. OPTIONS ENVISAGEES

Sans objet.

3.2. DISPOSITIF RETENU

Les présentes dispositions consacrent un renforcement du dispositif actuel afin de mieux encadrer les agents chargés de la supervision des opérateurs d'importance vitale, notamment s'agissant de leurs pouvoirs et des sanctions en cas d'obstacle au contrôle.

Il est ainsi prévu un dispositif d'assermentation, afin de consolider juridiquement les dossiers pouvant nourrir les procédures devant la Commission des sanctions instituée par l'article L. 1332-15 du présent projet de loi.

De même, sur le modèle de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, ou de la loi n° 2016-1691 du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique, les fonctions et prérogatives des agents en charge du contrôle sont encadrées et précisées.

Ainsi, ces agents de l'Etat, assermentés et habilités pour ce faire, peuvent réaliser des contrôles sur pièces et sur place, afin de vérifier la satisfaction par les OIV de leurs obligations.

A travers l'assermentation dont disposent ces agents, la sécurité juridique des conclusions de leurs enquêtes sera renforcée.

Des garanties sont présentes tant pour le respect de la législation de protection du secret que pour les intérêts économiques des opérateurs, notamment à travers le secret professionnel auquel ces agents sont strictement astreints, dans les conditions prévues à l'article 226-13 du code pénal. Cette condition parait en effet indispensable pour garantir aux opérateurs publics comme privés que les informations fournies aux agents chargés des contrôles ne pourront pas être utilisées à d'autres fins que celui du contrôle de la mise en œuvre du dispositif SAIV.

De même, par l'obligation de coopération des opérateurs avec les agents lors de la réalisation des contrôles, l'autorité administrative dispose d'une garantie supplémentaire pour assurer l'effectivité des règles de SAIV en vigueur. En cela, les présentes dispositions du projet de loi répondent pleinement aux objectifs de la directive REC, ainsi qu'aux objectifs de continuité des activités considérées comme « indispensables au fonctionnement de l'économie, de la société, à la défense, à la sécurité ou à la survie de la nation ». L'exonération limitée à l'Etat et à ses établissements publics administratifs se justifie par l'existence de moyens alternatifs à disposition des autorités administratives.

Toute manœuvre faisant obstacle au contrôle pourra être sanctionnée dans les mêmes conditions que celles concernant les obligations de résilience : la commission des sanctions sera alors saisie pour prononcer une telle sanction, sans que le cumul, le cas échéant, des sanctions pour les deux motifs ne puissent excéder le montant maximal prévu pour chacune des deux.

Enfin, pour assurer la dimension dissuasive et donc préventive du dispositif de contrôle, il est précisé que, le cas échéant et si les constations faites le nécessitent, la transmission au parquet se fait sans délai.

4. ANALYSE DES IMPACTS DES DISPOSITIONS ENVISAGEES

4.1. IMPACTS JURIDIQUES

4.1.1. Impact sur l'ordre juridique interne

La présente mesure crée les articles L. 1332-12 à L. 1332-14 du code de la défense au sein du chapitre II « Résilience des activités d'importance vitale », section 2 « Contrôles, sanctions administratives et dispositions pénales ».

4.1.2. Articulation avec le droit international et le droit de l'Union européenne

Les présentes dispositions ne correspondent pas à proprement parler d'une mesure de transposition de la directive REC. Néanmoins, cette dernière exige à son article 22 des Etats-membres qu'ils mettent en place des « mesures nécessaires (…), effectives, proportionnées et dissuasives » pour assurer le respect des dispositions induites par la directive elle-même.

Par ailleurs, la directive NIS2, qui s'applique également aux opérateurs identifiés comme critiques au sens de la directive, oblige les Etats membres dans ses articles 34 et 36 à mettre en place des sanctions administratives et pénales. Dans une logique de parallélisme, il a été décidé pour la transposition de la directive REC, de créer, en plus des sanctions pénales déjà existantes, des sanctions administratives.

En conséquence, les présentes dispositions permettent de mettre en cohérence le nouveau dispositif de contrôle des OIV avec la directive REC (notamment ses articles 21 et 22).

4.2. IMPACTS ECONOMIQUES ET FINANCIERS

4.2.1. Impacts macroéconomiques

Sans objet.

4.2.2. Impacts sur les entreprises

Sans objet.

4.2.3. Impacts budgétaires

Au-delà des efforts de réorganisation des priorités et de redéploiement des effectifs existants, les présentes dispositions pourraient conduire à recruter des ETP supplémentaires, notamment en préfecture, afin d'assurer l'application de l'ensemble des articles du futur chapitre II du titre III du Livre III de la partie I du code de la défense.

Il apparait essentiel, pour chaque ministère coordonnateur, d'identifier précisément les agents en charge des contrôles et ce, à tous les échelons impliqués : préfecture, zone de défense et ministères eux-mêmes (qu'il s'agisse des Services des hauts fonctionnaires de défense et de sécurité (SHFDS) ou d'autres services, par exemple ceux en charge de traiter les enquêtes administratives de sécurité).

Concrètement, pour les différents secteurs qui relèvent aujourd'hui de la sécurité des activités d'importance vitale, cela peut se traduire par des besoins en ressources humaines ou ressources budgétaires.

4.3. IMPACTS SUR LES COLLECTIVITES TERRITORIALES

Les opérateurs d'importance vitale qui seraient des collectivités territoriales seront tenues, comme pour les autres opérateurs, de donner accès aux locaux ainsi qu'aux données considérées comme nécessaires aux agents assermentés afin que ceux-ci s'assurent que les dispositions mises en œuvre par les opérateurs sont suffisantes au regard des obligations du code de la défense. Cette obligation ne devrait pas entrainer de frais supplémentaires pour les collectivités territoriales.

4.4. IMPACTS SUR LES SERVICES ADMINISTRATIFS

Les modalités de contrôle restent dans l'ensemble inchangées.

En revanche, les préfectures, dans le ressort desquelles se trouvent des OIV, pourraient être amenées à redéployer des effectifs ou à procéder à des recrutements d'ETP supplémentaires afin de pouvoir traiter les signalements effectués par les équipes de contrôle.

4.5. IMPACTS SOCIAUX

4.5.1. Impacts sur la société

Le renforcement des exigences en matière de sécurité des opérateurs d'importance vitale doit permettre de limiter les impacts sur le fonctionnement de la société d'une crise ou de problèmes majeurs touchant l'opérateur.

4.5.2. Impact sur les personnes en situation en handicap

Sans objet.

4.5.3. Impacts sur l'égalité entre les femmes et les hommes

Sans objet.

4.5.4. Impacts sur la jeunesse

Sans objet.

4.5.5. Impacts sur les professions réglementées

Sans objet.

4.6. IMPACTS SUR LES PARTICULIERS

Sans objet.

4.7. IMPACTS ENVIRONNEMENTAUX

Sans objet.

5. CONSULTATIONS MENEES ET MODALITES D'APPLICATION

5.1. CONSULTATIONS MENEES

Une concertation de l'ensemble des ministères coordonnateurs a été réalisée sur cette mesure.

En application de l'article L. 1212-2 du code général des collectivités territoriales, les présentes dispositions ont été soumises à l'examen du Conseil national d'évaluation des normes qui a rendu un avis défavorable le 22 mai 2024.

Enfin, le service national des enquêtes administratives de sécurité, le coordinateur général de la sécurité nucléaire, le service juridique du Secrétariat général des affaires européennes et l'Agence nationale de sécurité des systèmes d'informations ont également été consultés.

5.2. MODALITES D'APPLICATION

5.2.1. Application dans le temps

La présente disposition entre en vigueur le lendemain de la publication de la présente loi au *Journal officiel* de la République française. Toutefois, afin de produire des effets, elle nécessitera l'adoption d'un décret en Conseil d'Etat (mentionné *infra*).

5.2.2. Application dans l'espace

Conformément aux dispositions de l'article L. 1 du code de la défense, s'agissant d'une mesure liée à la politique de sécurité nationale ou à la politique de défense, la présente disposition s'appliquera de plein droit sur l'ensemble du territoire de la République, sans qu'aucune mention expresse d'application ne soit requise pour les collectivités d'outre-mer.

5.2.3. Textes d'application

Les présentes dispositions feront l'objet d'un décret en Conseil d'Etat, qui précisera la procédure de désignation et d'assermentation des agents de l'Etat.

Article 1er (L) – Articles L. 1332-15 à L. 1332-19 du code de la défense – Commission des sanctions

1. ETAT DES LIEUX

1.1. CADRE GENERAL

Le dispositif de sécurité des activités d'importance vitale repose sur une logique de coopération et de confiance entre l'Etat et les opérateurs d'importance vitale.

La finalité du dispositif est d'assurer, par les mesures de protection et de sécurité mises en œuvre par les opérateurs, un certain niveau de résilience des entités désignées opérateurs d'importance vitale.

L'objectif final reste en effet la continuité d'activité des activités d'importance vitale. Un certain niveau de souplesse est donc à mettre en place dans le suivi du dispositif, qui ne se veut pas coercitif. C'est pourquoi le dispositif se met en œuvre avec une logique de résultats et non pas de moyens : c'est à l'opérateur, par les plans de résilience qu'il effectue, de prouver à l'autorité étatique que son dispositif ainsi que les mesures de résilience qu'il met en place sont suffisantes pour assurer la continuité de sa ou ses activités d'importance vitale.

La législation actuelle ne comporte donc que très peu de dispositions permettant la mise en œuvre de sanctions, qu'elles soient administratives ou pénales.

Sanctions administratives du dispositif

Plusieurs dispositions existent aujourd'hui dans le code de la défense permettant à l'autorité administrative de prendre certaines mesures administratives à l'encontre d'un opérateur d'importance vitale qui ne remplirait pas ses obligations.

En effet, l'article L. 1332-4 de l'actuel code de la défense permet à l'autorité administrative – le préfet de département ou l'autorité militaire compétente – de mettre par arrêté « en cas de refus des opérateurs de préparer leur plan particulier de protection, […], les chefs d'établissements ou d'entreprises assujettis en demeure de l'établir dans le délai qu'elle fixe ».

Cette autorité administrative a la possibilité, en vertu de l'article L. 1332-5 de ce même code, de mettre ces mêmes chefs d'établissements ou d'entreprises assujettis en demeure de réaliser le plan particulier de protection, dont l'obligation est régie à l'article L. 1332-3.

L'actuel article L. 1332-6 du code de la défense clarifie les modalités de mises en œuvre des dispositions précédentes :

« Les arrêtés de mise en demeure prévus aux articles L. 1332-4 et L. 1332-5 fixent un délai qui ne peut être inférieur à un mois, et qui est déterminé en tenant compte des conditions de fonctionnement de l'opérateur et des travaux à exécuter.

Les arrêtés concernant les entreprises nationales ou faisant appel au concours financier de l'Etat sont transmis au ministre de tutelle et au ministre de l'économie et des finances, qui sont immédiatement informés des difficultés susceptibles de se produire dans l'application de l'arrêté ».

Dans les faits, ces mesures n'ont jamais été réalisées, des solutions privilégiant le dialogue entre l'autorité administrative et l'opérateur étant mises en œuvre.

Sanctions pénales du dispositif

L'actuel article L. 1332-7 du dispositif donne aujourd'hui une base juridique à la SAIV pour mettre en œuvre s'il y a lieu des sanctions pénales. Les manquements sur lesquels peuvent porter les sanctions sont les suivants :

- non-réalisation du plan particulier de protection dans les délais impartis par l'arrêté de mise en demeure évoqué au L. 1332-4 ;
- absence d'entretien des dispositifs de protection malgré une mise en demeure ;
- non-respect des obligations relatives à la cybersécurité du dispositif (articles L. 1332-6-1 à L. 1332-6-4 du code de la défense, avec une mise en demeure devant être effectuée au préalable).

Les personnes susceptibles d'encourir ces sanctions pénales, avec une amende de 150 000 euros, sont pour ces trois cas de figure les chefs d'établissements ou d'entreprises assujettis.

Les personnes morales peuvent également être déclarées responsables. L'actuel article L. 1332-7 du code de la défense dispose en effet que, dans les conditions prévues à l'article L. 121-2 du code pénal, « des infractions prévues au [L. 1332-7] encourent une amende suivant les modalités prévues à l'article 131-38 du même code ».

Dans les faits, aucune sanction pénale n'a jamais été prononcée en vertu du dispositif de sécurité des activités d'importance vitale. Ce constat s'explique par le fait que, comme expliqué *supra*, la mise en œuvre du dispositif se fait avant tout dans une logique de coopération et de confiance entre l'Etat et l'opérateur. La mise en œuvre de sanctions n'est pas l'objectif de cette politique publique. De plus, les contraintes techniques mises en œuvre sur le dispositif, dont la plupart des informations y faisant référence sont classifiées par la protection du secret de la défense nationale – sont donc par nature difficiles à divulguer, même au travers d'une procédure pénale. Il faudrait en effet que les personnes soient habilitées au secret de la défense nationale et aient le besoin d'en connaitre.

1.2. CADRE CONSTITUTIONNEL

Aux termes de l'article 88-1 de la Constitution : « La République participe aux Communautés européennes et à l'Union européenne, constituées d'Etats qui ont choisi librement, en vertu des traités qui les ont instituées, d'exercer en commun certaines de leurs compétences ». Le Conseil constitutionnel déduit de cette disposition que : « la transposition en droit interne d'une directive communautaire résulte d'une exigence constitutionnelle »[101]. Il en va de même pour une loi ayant pour objet d'adapter le droit interne à un règlement de l'Union européenne[102].

Les dispositions applicables aux entités critiques et le régime de sanction lié portent nécessairement une atteinte à la liberté d'entreprendre, laquelle découle de l'article 4 de la Déclaration des droits de l'Homme et du Citoyen de 1789[103]. Cette atteinte ne peut être ni générale ni absolue[104]. Le législateur peut limiter l'exercice de cette liberté à la condition qu'il n'en résulte pas d'atteintes disproportionnées au regard de l'objectif poursuivi[105], alors même que cette atteinte résulterait de l'exigence constitutionnelle de transposition adéquate des directives européennes[106], dans un objectif de sécurité et de défense de la Nation, en l'absence de disposition spécifique contraire de la Constitution[107] ou de mise en cause d'une règle ou d'un principe inhérent à notre identité constitutionnelle[108].

Enfin, en l'absence de remise en cause de ses garanties fondamentales, la liberté du commerce et de l'industrie ne s'oppose pas à l'intervention du législateur dans ce domaine[109].

Par ailleurs, s'agissant du cadre constitutionnel applicable aux dispositions prévoyant des sanctions administratives, il a été rappelé par la jurisprudence constitutionnelle « qu'aucun principe ou règle de valeur constitutionnelle ne fait obstacle à ce qu'une autorité administrative non soumise au pouvoir hiérarchique du ministre, agissant dans le cadre de prérogatives de puissance publique, puisse exercer un pouvoir de sanction »[110]. Ainsi, une commission qui n'est pas légalement une autorité administrative indépendante peut tout de

---

[101] Voir notamment la décision n° 2004-496 DC du 10 juin 2004, « Loi pour la confiance dans l'économie numérique ».

[102] Voir par exemple la décision n° 2018-765, « Loi relative à la protection des données personnelles », considérant 3.

[103] Conseil constitutionnel, décision 98-401 DC du 10 juin 1998.

[104] Décision 82-141 DC du 27 juillet 1982.

[105] Décision 2023-1055 QPC du 16 juin 2023.

[106] Décision 2006-535 DC du 30 mars 2006.

[107] Décision 2004-497 DC du 1er juillet 2004.

[108] Décision 2018-765 DC du 12 juin 2018 ; décision 2019-818 QPC du 6 décembre 2019.

[109] Décision 2003-474 DC du 17 juillet 2003.

[110] Décision 2016-616, 617 QPC du 9 mars 2017.

même infliger des sanctions administratives dès lors que sont respectées les garanties d'indépendance et d'impartialité et que la procédure instituée respecte les exigences qui s'imposent en tel domaine (droits de la défense principalement pour les sanctions ayant le caractère de punition[111]).

Sur la nature et le montant des sanctions susceptibles d'être prononcées après contrôle et constatation de manquements par un agents assermenté, donc par une autre autorité que la commission dans le respect du principe de séparation des poursuites et du jugement[112], celles-ci doivent respecter des règles de fond semblables à celles prévalant en matière pénale dès lors que ces sanctions ont vocation à punir la méconnaissance de règles d'exercice d'une activité.

Il en est ainsi du principe de nécessité[113] et de proportionnalité[114], du principe de légalité, du principe d'individualisation, lesquels principes d'appuient sur des définitions précises d'infractions pouvant être sanctionnées[115].

Il en résulte un encadrement constitutionnel fort et nécessaire de toute sanction administrative pouvant être infligée à un opérateur par une commission indépendante ne relevant pas du pouvoir hiérarchique d'un ministre mais n'étant pas légalement une autorité administrative indépendante.

1.3. CADRE CONVENTIONNEL

La directive européenne résilience des entités critiques (REC), dans ses articles 21 et 22, impose aux Etats membres d'avoir les moyens nécessaires de vérifier que les opérateurs désignés mettent bien en œuvre les dispositions de résilience prévues dans la directive – en particulier au titre de l'article 13.

Il est en effet spécifié à l'article 21-1 de la directive que :

« Afin d'évaluer le respect des obligations découlant de la présente directive par les entités qu'ils ont recensées en tant qu'entités critiques en vertu de l'article 6, paragraphe 1, de la présente directive, les Etats membres veillent à e que les autorités compétentes disposent des pouvoirs et des moyens nécessaires pour :

[111] Décision 2017-688 QPC du 2 février 2018.

[112] A contrario, décision 2017-675 QPC du 24 novembre 2017.

[113] Décision 2021-953 QPC du 3 décembre 2021.

[114] Décision 2022-988 QPC du 8 avril 2022.

[115] Décision 2013-332 QPC du 12 juillet 2013.

a) « Procéder à des inspections sur place de l'infrastructure critique et des locaux utilisés par l'entité critique pour fournis ses services essentiels et à la supervision à distance des mesures prises par les entités critiques conformément à l'article 13 ;

b) Effectuer ou ordonner des audits portant sur ces entités critiques ».

Sur la directive résilience des entités critiques, les Etats membres ont peu d'indications sur les sanctions qu'ils sont supposés mettre en œuvre – le législateur européen ayant fait le choix de laisser les Etats membres décider des dispositions qui leur paraitraient les plus opportunes. En effet l'article 22 de la directive stipule que :

« Les Etats membres déterminent le régime de 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. Ces sanctions doivent être effectives, proportionnées et dissuasives. Les Etats membres informent la Commission, au plus tard le 17 octobre 2024 du régime ainsi déterminé et des mesures ainsi prises, de même que, sans retard, de toute modification apportée ultérieurement à ce régime ou à ces mesures ».

1.4. ELEMENTS DE DROIT COMPARE

Sans objet.

2. NECESSITE DE LEGIFERER ET OBJECTIFS POURSUIVIS

2.1. NECESSITE DE LEGIFERER

La modernisation du dispositif ne doit pas entraîner un changement de logique dans son application : l'objectif n'est pas de sortir de la logique de coopération et de confiance mise en œuvre entre l'Etat et les opérateurs et de mettre en place un nombre important de sanctions.

Les Etats membres ont la possibilité de mettre en place le régime de sanctions qui leur parait le plus pertinent, qu'il soit composé de sanctions administratives, pénales ou les deux. Toutefois, il faut rappeler que les entités critiques désignées au titre de l'application de la directive – donc les opérateurs d'importance vitale qui seront désignés sur le fondement du deuxième alinéa du 1° du I de l'article L. 1332-2 car fournissant des services essentiels au

sens de la directive – sont également des entités essentielles pour la directive NIS2[116]. Or, pour cette directive, les sanctions prévues sont beaucoup plus prescriptives.

L'article 34 de la directive NIS2 prévoit en effet que les entités essentielles puissent être soumises à des amendes administratives d'un montant maximal s'élevant à 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. L'article 32 de cette même directive, qui prévoit les mesures de supervision et d'exécution en ce qui concerne les entités essentielles, est également largement prescriptif.

Etant donné que la désignation en tant qu'opérateur d'importance vitale, en vertu de sa désignation au titre du nouveau L. 1332-2 entraîne la désignation de l'entité comme entité essentielle – ce point est prévu dans l'article de la présente loi qui fixe les conditions de désignation des entités essentielles. Les opérateurs d'importance vitale seront donc soumis aux sanctions administratives prévues par la directive NIS2.

Dans une logique de cohérence, il apparait opportun de renforcer le niveau de sanctions possibles sur la dimension physique du dispositif SAIV afin de ne pas créer de distorsion flagrante entre les sanctions encourues pour des manquements physiques par rapport à ceux de la dimension cyber.

Cette disposition s'appliquera de plus à tous les opérateurs d'importance vitale, car comme expliqué *supra* dans la partie de l'étude d'impact relative à l'article L. 1332-11, les dispositions relevant de la protection cyber imposées aux opérateurs d'importance vitale seront identiques pour tous les secteurs d'activité – que ceux-ci soient concernés par la liste des services essentiels de la directive REC ou non. Dans cette même logique, les sanctions mises en œuvre au titre de la sécurité des activités d'importance vitale seront uniques pour tous les secteurs d'activités d'importance vitale.

Etant donné les éléments évoqués précédemment, il est apparu opportun de créer une entité chargée du suivi des sanctions administratives, sachant que ladite entité devait fournir un certain nombre de garanties, que ce soit en termes de traitement, d'équité et d'impartialité, auprès des opérateurs assujettis. Cette instance doit pouvoir être destinataire des informations, rapports de contrôle effectués par la ou les autorités administratives en charge du suivi des opérateurs d'importance vitale, tout en gardant une indépendance par rapport aux autorités en charge du contrôle.

[116] 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 NIS 2).

L'introduction dans la loi de cette nouvelle entité parait indispensable en ce qu'elle constitue une garantie essentielle s'agissant de la possibilité de sanctionner la méconnaissance de dispositions législatives par un opérateur.

2.2. OBJECTIFS POURSUIVIS

L'objectif du présent article est de créer une autorité compétente chargé d'émettre, s'il y a lieu et en cas de manquement établi, des sanctions administratives. A ce titre, cette entité doit être indépendante des autorités en charge du contrôle, afin d'assurer un certain nombre de garanties aux opérateurs d'importance vitale.

Les sanctions administratives doivent de plus être uniformes entre les différents secteurs d'activité d'importance vitale, il apparaissait donc peu opportun de laisser les autorités administratives responsables de chaque secteur d'activité d'être les seuls à décider sur leurs opérateurs d'importance vitale. Une entité rattachée au Premier ministre, pouvant traiter des différents cas des secteurs d'activités d'importance vitale, paraissait idoine afin d'assurer l'égalité de traitement entre les opérateurs.

L'objectif est également de faire en sorte que les sanctions prises par cette entité puissent être éclairées, avec des personnes ayant une connaissance de la thématique et des obligations imposées aux opérateurs.

3. OPTIONS ENVISAGEES ET DISPOSITIF RETENU

3.1. OPTIONS ENVISAGEES

Lors des consultations effectuées avec les ministères coordonnateurs dans le cadre des travaux de transposition de la directive REC, a été évoqué la possibilité de donner les pouvoirs de supervision et de contrôle des opérateurs d'importance vitale à ces seuls ministères. Les sanctions administratives auraient donc été prises pour tous les opérateurs d'importance vitale par le ministère coordonnateur responsable du secteur d'activité au titre duquel l'opérateur a été désigné. Cette solution ne paraissait pas idéale pour plusieurs raisons :

- Les possibilités de différences de traitement entre les différents ministères sur leurs opérateurs pouvaient créer des distorsions de traitement et donc une inégalité entre les opérateurs désignés ;
- Pour les opérateurs pouvant être désignés au titre de plusieurs secteurs d'activités d'importance vitale, une coordination interministérielle se serait avérée nécessaire ;

Ces différentes raisons ont fait apparaitre la nécessité de créer une instance impartiale et équitable pour tous les opérateurs sur ces sujets, et qui permettent un suivi uniforme et interministériel de la SAIV sur l'ensemble du territoire.

Une fois l'option de la commission retenue, il s'est posé la question de la nature et de la composition de cette commission.

Afin de rendre le dispositif le plus efficace et le plus adapté au domaine particulier de la SAIV, il a été écarté toute possibilité de créer une nouvelle autorité administrative indépendante ou tout autre organe revêtant les caractéristiques d'une juridiction.

3.2. DISPOSITIF RETENU

Le présent article crée une commission placée auprès du Premier ministre en charge du traitement et de la prononciation des sanctions administratives pouvant être émises sur les opérateurs d'importance vitale.

A ce titre, il est prévu qu'elle soit compétente pour constater des manquements en vertu des obligations créées par le présent chapitre. La saisine de cette commission ne pourra être faite que par les autorités administratives chargées d'effectuer les contrôles au titre des articles L. 1332-12 et L. 1332-13. Pour le dispositif de sécurité des activités d'importance vitale, il pourra s'agir des ministères coordonnateurs, les préfectures de département ou autorité militaire compétente, ou les zones de défense et de sécurité. Les modalités de saisine devront être clarifiées par voie réglementaire.

Afin de pouvoir prendre une décision éclairée, la commission reçoit les rapports et procès-verbaux des contrôles. Une fois saisie, il est prévu qu'elle notifie à l'opérateur les griefs susceptibles d'être retenus à son encontre.

La composition de la Commission est mentionnée à l'article L. 1332-16. Elle doit être composée d'un membre du Conseil d'Etat désigné par le vice-président du Conseil d'Etat, d'un membre de la Cour de cassation désigné par le président de cette même Cour, d'un membre de la Cour des comptes désigné par le premier président de la Cour des comptes. De plus, trois personnalités qualifiées sont désignées pour être membre de la Commission : ces personnes doivent être désignées en vertu de leur compétence dans le domaine de la sécurité des activités d'importance vitale, sur proposition de l'autorité administrative.

Il est rappelé que les membres de cette commission doivent prendre leur décision en toute impartialité : ils ne peuvent recevoir d'instructions de la part d'aucune autorité. Afin d'assurer le suivi du dossier, un rapporteur est nommé, sans possibilité pour ce rapporteur de recevoir aucune instruction. La décision prise doit être motivée, et ne peut être donnée sans que l'opérateur n'ait été entendu ou, à défaut, dûment convoqué. Elle a la possibilité d'auditionner

toute personne qu'elle juge utile. La décision est prise à la majorité des membres présent : en cas de partage des voix, celle du président est prépondérante.

Les amendes administratives (L. 1332-17) pouvant être prises par la Commission peuvent aller jusqu'à 10 millions d'euros ou 2% du chiffre d'affaires annuel mondial (obligation liée à l'article 34 de la directive NIS2). Une amende peut également être réalisée par la Commission dans le cas où l'opérateur d'importance vitale ferait obstacle aux demandes de l'autorité administrative dans le cadre des contrôles effectués (obligation du L. 1332-13).

Les opérateurs d'importance vitale qui seraient des administrations de l'Etat, des collectivités territoriales et de leurs établissements publics administratifs, ne sont pas soumis à l'amende mentionnée supra.

La commission des sanctions peut également prendre des sanctions administratives en vertu de certaines obligations prévues aux articles 28 et 37 du présent projet de loi.

L'entité chargée d'émettre les sanctions (L. 1332-18) a la possibilité d'ordonner la publication, la diffusion, l'affichage de la sanction pécuniaire ou d'un extrait. Les modalités de recouvrement de ces sanctions sont également présentées dans le présent article, ainsi que les possibilités de recours.

4. ANALYSE DES DISPOSIITONS ENVISAGEES

4.1. IMPACTS JURIDIQUES

4.1.1. Impact sur l'ordre juridique interne

Des articles L. 1332-15 à L. 1332-19 sont créés dans le code de la défense, au sein de la nouvelle sous-section 2 « Sanctions » de la Section 2 « Contrôles et sanctions administratives ».

Ces dispositions sont proportionnées et en rapport avec l'objectif poursuivi se rattachant à la défense et à la sécurité nationale.

4.1.2. Articulation avec le droit international et le droit de l'Union européenne

Les présentes dispositions du projet de loi permettent d'assurer la cohérence du droit français avec les articles 21 et 22 de la directive REC ainsi que les articles 34 et 36 de la directive NIS2.

4.2. IMPACTS ECONOMIQUES ET FINANCIERS

4.2.1. Impacts macroéconomiques

Sans objet.

4.2.2. Impacts sur les entreprises

L'impact ne pourra porter que sur les opérateurs d'importance vitale, soit un peu moins de 400 entités en France.

Les possibilités de sanctions sont relativement importantes et pourraient impacter fortement les opérateurs, mais les amendes prises devront prendre en compte les capacités financières de l'opérateur. Il serait contreproductif que des sanctions visant à obliger à un opérateur à se conformer aux obligations de la sécurité des activités d'importance vitale aient pour conséquence de l'empêcher financièrement de mettre en place ces mesures. L'objectif de la sécurité des activités d'importance vitale reste d'assurer la continuité d'activité d'opérateur qui fournissent des services ou activités considérés comme essentiels par l'Etat ou la Nation.

De plus, il est rappelé que la logique de coopération et de confiance entre l'Etat et l'opérateur est indispensable pour la bonne mise en œuvre du dispositif. La mise en place d'une procédure de sanctions devra rester l'exception plutôt que la norme, et impacter un nombre limité d'opérateurs.

4.2.3. Impacts budgétaires

La mise en œuvre de la procédure ainsi que le traitement des dossiers impactera les services administratifs compétents. Dans une même logique que ce qui a pu être indiqué dans les briques de l'étude d'impact *supra* relatives aux articles L. 1332-12 et L. 1332-13, un renforcement en matière de ressources humaines des services administratifs en charge du suivi des contrôles et rapports effectués auprès des opérateurs pourrait être nécessaire, et favoriserait plus largement le suivi du dispositif de sécurité des activités d'importance vitale.

4.3. IMPACTS SUR LES COLLECTIVITES TERRITORIALES

Les collectivités territoriales peuvent faire partie des 400 entités concernées.

Une disposition expresse du présent article exclut les collectivités territoriales, qui ne pourront se voir infliger d'amendes administratives de la part de la Commission des sanctions.

4.4. IMPACTS SUR LES SERVICES ADMINISTRATIFS

Sans objet. Comme mentionné au 4.2.3. *supra*, un renforcement en matière de ressources humaines des services administratifs en charge du suivi des contrôles et rapports effectués auprès des opérateurs pourrait être nécessaire.

4.5. IMPACTS SOCIAUX

4.5.1. Impacts sur la société

Le renforcement des exigences en matière de sécurité des opérateurs d'importance vitale doit permettre de limiter les impacts sur le fonctionnement de la société d'une crise ou de problèmes majeurs touchant l'opérateur.

4.5.2. Impact sur les personnes en situation en handicap

Sans objet.

4.5.3. Impacts sur l'égalité entre les femmes et les hommes

Sans objet.

4.5.4. Impacts sur la jeunesse

Sans objet.

4.5.5. Impacts sur les professions réglementées

Sans objet.

4.6. IMPACTS SUR LES PARTICULIERS

Sans objet.

4.7. IMPACTS ENVIRONNEMENTAUX

Sans objet.

5. CONSULTATIONS MENEES ET MODALITES D'APPLICATION

5.1. CONSULTATIONS MENEES

Une concertation a été réalisée avec l'ensemble des ministères coordonnateurs et l'Agence Nationale de la Sécurité des Systèmes d'information (ANSSI).

En application de l'article L. 1212-2 du code général des collectivités territoriales, les présentes dispositions ont été soumises à l'examen du Conseil national d'évaluation des normes qui a rendu un avis défavorable le 22 mai 2024.

Enfin, le service national des enquêtes administratives de sécurité, le coordinateur général de la sécurité nucléaire, le service juridique du Secrétariat général des affaires européennes et l'Agence nationale de sécurité des systèmes d'informations ont également été consultés.

5.2. MODALITES D'APPLICATION

5.2.1. Application dans le temps

Les présentes dispositions entreront en vigueur le lendemain de la publication de la présente loi au *Journal officiel* de la République française. Toutefois, afin de produire des effets, elles nécessiteront l'adoption d'un décret en Conseil d'Etat (mentionné *infra, 5.2.3.*).

5.2.2. Application dans l'espace

Conformément aux dispositions de l'article L. 1 du code de la défense, s'agissant d'une mesure liée à la politique de sécurité nationale ou à la politique de défense, les présentes dispositions s'appliqueront de plein droit sur l'ensemble du territoire de la République, sans qu'aucune mention expresse d'application ne soit requise pour les collectivités d'outre-mer.

5.2.3. Textes d'application

Les présentes dispositions feront l'objet d'un décret en Conseil d'Etat.

Article 1er (M) – Article L. 1332-20 à L. 1332-22 du code de la défense – Marchés publics et contrats de concessions relatifs à la sécurité des activités d'importance vitale

1. ETAT DES LIEUX

1.1. CADRE GENERAL

L'évolution de la situation internationale, notamment la guerre en Ukraine, est venue rappeler l'importance de la sécurité des infrastructures critiques indispensables au fonctionnement de la Nation, parfaitement susceptibles de subir l'ingérence de puissances qui pourraient être hostiles à nos intérêts ou le devenir dans un contexte international mouvant.

Ce risque d'ingérence n'est pas limité aux États, il peut également être le fait d'entreprises qui y sont liées et pourraient, en particulier en cas de conflit ou de tensions internationales, chercher à perturber certaines activités d'importance vitale ou encore à exploiter des informations qu'elles tiendraient de leurs interventions passées pour le compte d'un OIV.

Il apparaît donc nécessaire de garantir notre maîtrise sur les entreprises qui seraient en mesure d'affecter la sécurité des OIV et la continuité de leurs activités.

En l'état actuel du droit, il n'existe pas réellement de moyen de se prémunir du risque qu'un acteur hostile, ou soupçonné de l'être, candidate à des marchés ou des concessions, voire les remporte en application des règles de la consultation lorsque ces marchés ou ces concessions sont passés en application du code de la commande publique.

Le code de la commande publique prévoit certes des dispositions permettant de limiter l'accès aux marchés publics aux opérateurs émanant d'États qui n'ont pas signé l'accord sur les marchés publics de l'OMC, notamment dans ses articles L. 2153-1 et L. 2153-2. Mais ces dispositions issues des directives européennes, bien qu'elles représentent une avancée positive, ont été conçues comme des instruments de réciprocité commerciale et pas comme des instruments de protection de nos intérêts essentiels. Elles sont par ailleurs peu protectrices puisque les filiales européennes de groupes étrangers doivent être traitées comme des entreprises européennes.

Le règlement 2022/1031 dit « IMPI » (Instrument relatif aux marchés publics internationaux)[117] représente une évolution favorable de ce point de vue, puisqu'il permet

[117] Règlement (UE) 2022/1031 du Parlement européen et du Conseil du 23 juin 2022 concernant l'accès des opérateurs économiques, des biens et des services des pays tiers aux marchés publics et aux concessions de l'Union et établissant des procédures visant à faciliter les négociations relatives à l'accès des opérateurs

d'assimiler une filiale sans activité substantielle dans l'UE à une société étrangère. Cependant, ce règlement est, là encore, destiné à régler des questions de réciprocité dans l'ouverture des marchés, et ne vise pas à traiter des questions de protection des intérêts essentiels de la Nation. Sa mise en œuvre relève par ailleurs de la Commission, et non des États membres.

La protection de nos intérêts essentiels doit donc s'inscrire dans le cadre prévu spécifiquement à cet effet.

Le droit de la commande publique offre, sous certaines conditions, plusieurs outils mobilisables par les OIV afin d'alléger les obligations qu'ils doivent respecter lors de la passation de leurs marchés.

Ainsi, certains OIV[118] peuvent recourir aux marchés de défense ou de sécurité, définis à l'article L. 1113-1 du code de la commande publique, qui, en fonction de leur objet, sont exemptés des obligations de publicité et de mise en concurrence ou sont soumis à des obligations adaptées à leurs spécificités. La mise en œuvre de ces dispositifs ne peut, cependant, être ni générale ni automatique et doit résulter d'une démonstration au cas par cas par l'acheteur. Le Conseil d'Etat a ainsi récemment rappelé[119] que la seule circonstance que les sites concernés par le marché constituaient des points d'importance vitale n'était pas de nature à imposer que toute prestation en lien avec ces sites devait être considérée comme bénéficiant de dérogations prévues par le CCP.

Surtout, 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 conformément aux dispositions législatives ou réglementaires en vigueur ou pour lesquels la protection des intérêts essentiels de l'État l'exige, à condition que cette sécurité ou cette protection ne puisse pas être garantie par d'autres moyens (article L. 2512-3). Le code prévoit des dispositions analogues pour les contrats de concessions : ceux qui exigent le secret ou dont l'exécution doit s'accompagner de mesures particulières de sécurité conformément aux dispositions législatives ou réglementaires en vigueur ou pour lesquels la protection des intérêts essentiels de l'État l'exige, à condition que cette sécurité ou cette protection ne puisse pas être garantie par

économiques, des biens et des services originaires de l'Union aux marchés publics et aux concessions des pays tiers (Instrument relatif aux marchés publics internationaux — IMPI).

[118] Depuis l'entrée en vigueur de la loi n° 2018-607 du 13 juillet 2018 relative à la programmation militaire pour les années 2019 à 2025 et portant dispositions intéressant la défense, le champ d'application des marchés de défense ou de sécurité, qui était limité à l'État et ses établissements publics ayant un caractère autre qu'industriel et commercial, a été étendu à l'ensemble des établissements publics de l'État (article L. 1113-1 du code de la commande publique).

[119] Conseil d'Etat, n° 445396, Ministre des armées c/ Société OSR, 4 février 2021. Voir notamment les conclusions de Mme LE CORRE, rapporteure publique.

d'autres moyens, sont soumis au seul titre II du livre II de la troisième partie du code de la commande publique (article L. 3212-3).

Ce régime correspond à celui des marchés et concessions qui étaient exclus du champ d'application de l'ancien code des marchés publics et de l'ordonnance n° 2016-65 du 29 janvier 2016 relative aux contrats de concession, et qui peuvent donc notamment être conclus sans mise en concurrence et sans publicité.

Il trouve son pendant, en droit européen, dans les dispositions de l'article 15 de la directive 2014/2433[120] pour les pouvoirs adjudicateurs et de l'article 24 de la directive 2014/25[121] pour ce qui concerne les entités adjudicatrices opérant dans le secteur de l'électricité.

La présente mesure vise à en clarifier les conditions d'application à certains marchés et concessions des OIV.

1.2. CADRE CONSTITUTIONNEL

La liberté et l'égalité d'accès à la commande publique sont des principes de valeur constitutionnelle[122].

Ils doivent être combinés avec les autres principes à valeur constitutionnelle, notamment la sauvegarde des intérêts fondamentaux de la Nation, au nombre desquels figurent l'indépendance de la Nation ainsi que les éléments essentiels de son potentiel économique[123] .

Le Conseil constitutionnel a par exemple confirmé à cet égard que les réacteurs électronucléaires à construire participent de ces éléments essentiels du potentiel économique[124].

1.3. CADRE CONVENTIONNEL

L'article III de l'accord sur les marchés publics[125] de l'OMC prévoit que : « rien dans le présent accord ne sera interprété comme empêchant une Partie quelconque d'entreprendre une

[120] Directive 2014/23/UE du Parlement européen et du Conseil du 26 février 2014 sur l'attribution de contrats de concession.

[121] 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.

[122] Conseil constitutionnel, décision n°2003-473 DC du 26 juin 2003.

[123] Conseil constitutionnel, décision n° 2015-713 DC du 23 juillet 2015 ; Conseil constitutionnel, décision n° 2022-843 DC du 12 août 2022.

[124] Conseil constitutionnel, décision n° 2023-851 DC du 21 juin 2023, §28.

action ou de ne pas divulguer des renseignements si elle l'estime nécessaire à la protection des intérêts essentiels de sa sécurité, se rapportant aux marchés d'armes, de munitions ou de matériel de guerre, ou aux marchés indispensables à la sécurité nationale ou aux fins de la défense nationale ».

En droit européen, les directives relatives à la commande publique mentionnée *supra* prévoient en conséquence une exclusion de leur application pour des raisons de sécurité, notamment « dans la mesure où la protection des intérêts essentiels de la sécurité d'un État membre ne peut être garantie par des mesures moins intrusives » (article 10 de la directive 2014/23, article 15 de la directive 2014/24 et article 24 de la directive 2014/25).

La jurisprudence européenne et la Commission ont confirmé que les « intérêts essentiels » de la sécurité de l'État ne se limitent pas aux intérêts de la défense nationale ou de la sécurité au sens le plus étroit du terme.

La Commission a ainsi estimé que la Lituanie avait pu attribuer sans mise en concurrence la construction et l'exploitation d'un terminal de gaz naturel liquéfié, et considéré que l'absence de mise en concurrence était appropriée et proportionnée au but poursuivi au regard des enjeux de sécurité énergétique pour éviter tout lien entre le titulaire du contrat et un opérateur étranger, que ce soit à l'occasion de son attribution ou à l'avenir (Commission européenne, 20 novembre 2013, décision SA.36740, §229 et suivants).

Cette décision de la Commission a été validée par le tribunal de l'Union européenne (TUE, 12 septembre 2019, aff. T. 417/16, notamment points 128 et suivants).

Le Tribunal a notamment jugé qu'aucune mesure autre que l'attribution directe n'aurait pu garantir la sécurité d'approvisionnement, et a considéré que d'autres solutions d'une nature moins restrictive telles que, par exemple, les critères d'attribution, l'imposition d'obligations pouvant être assorties de sanctions pénales, l'insertion d'exigences en matière de sécurité dans le contrat ou l'examen de la capacité à respecter certaines exigences en matière de capacité technique n'auraient pas permis de garantir la protection des intérêts essentiels de la Lituanie.

Le Tribunal a également confirmé à cette occasion que l'exception relative à la protection des intérêts essentiels de l'État s'applique tant sous l'empire des directives relatives à la commande publique que sous l'empire des grands principes issus des traités et qu'elle permet ainsi de procéder par voie d'attribution directe, sans aucune forme de publicité ni de mise en concurrence (§132).

Cette décision a été confirmée par la Cour de justice de l'Union européenne (CJUE, 29 avril 2021, aff. C-847/19 P, notamment pts. 58 et s.).

---

[125] https://www.wto.org/french/tratop_f/gproc_f/gp_gpa_f.htm.

La Cour de justice a notamment consacré dans sa décision l'existence d'une « marge d'appréciation » laissée aux États membres pour décider des mesures jugées nécessaires à la protection des intérêts essentiels de leur sécurité.

Dans le même sens, la Commission a admis l'inapplicabilité des directives relatives aux marchés publics dans le cas de la centrale nucléaire de Dukovany en République Tchèque sur le fondement des intérêts essentiels de l'État (Décision de la Commission SA.58207, §169 et s.).

En dehors du domaine énergétique, la Cour de justice a également admis récemment le recours à cette exception pour l'impression de certains documents par la Pologne (CJUE 7 septembre 2023, aff. C-601/21).

Cette décision rappelle notamment que l'objectif de préservation de la sécurité nationale correspond « à l'intérêt primordial de protéger les fonctions essentielles de l'État et les intérêts fondamentaux de la société, par la prévention et la répression des activités de nature à déstabiliser gravement les structures constitutionnelles, politiques, économiques ou sociales d'un pays ». Elle a admis le recours à l'exception tirée de la protection des intérêts essentiels au motif que certains documents présentaient un niveau de sensibilité particulièrement élevé et qu'une éventuelle fuite pourrait avoir des conséquences irréparables pour la sécurité nationale. Elle a enfin confirmé que le droit de l'Union n'impose pas de contrainte aux États membres quant au niveau de protection de leurs intérêts essentiels qu'ils souhaitent atteindre.

La possibilité d'attribution directe est conforme à la jurisprudence de la Cour, qui reconnaît qu'il peut être dérogé au principe de transparence pour des raisons impérieuses d'intérêt général ; pour un motif énoncé à l'article 52 du TFUE (qui vise notamment la sécurité publique) ou, plus largement, pour des « *considérations prises en compte par le droit de l'Union* ».

En droit interne, la position du Conseil d'Etat sur les services juridiques va dans le même sens puisqu'elle évoque une « dérogation »[126] aux principes dégagés par le Conseil constitutionnel. Le Conseil constitutionnel a également admis[127] la constitutionnalité des dispositions du code de la commande publique qui permettent de conclure des contrats sans publicité ni mise en concurrence lorsqu'un motif d'intérêt général le justifie (au sujet de l'article L. 2122-1 du code de la commande publique qui permet notamment de prévoir une procédure sans publicité

[126] Avis du Conseil d'Etat du 27 septembre 2018 sur le projet de loi relatif à la suppression des surtranspositions des directives européennes en droit français : « *[…] le Conseil d'État estime que la spécificité de ces services juridiques peut autoriser, en raison d'un motif d'intérêt général directement lié à la nécessité de tenir compte des caractéristiques propres à de tels services eu égard notamment au principe de libre choix de l'avocat et à l'importance de l'intuitu personae en la matière, une dérogation aux principes fondamentaux de la commande publique que le Conseil constitutionnel a dégagés dans sa décision n° 2003-473 DC du 26 juin 2003* ».

[127] Conseil constitutionnel, décision n° 2020-807 DC du 3 décembre 2020 sur la loi d'accélération et de simplification de l'action publique.

ni mise en concurrence à raison de l'objet du marché quand le respect d'une telle procédure est contraire à un motif d'intérêt général). Or la sauvegarde du potentiel économique de la Nation est déjà reconnue comme un principe de valeur constitutionnelle.

1.4. ELEMENTS DE DROIT COMPARE

Il apparaît que d'autres pays européens ont déjà encouragé les acheteurs publics à faire usage des dispositions dérogatoires prévues par les articles 15 de la directive 2014/24 et 24 de la directive 2014/25, parfois sans recourir à un vecteur législatif qui en préciserait le champ d'application exact.

S'agissant de la Belgique, par exemple, l'article 33 de sa loi sur les marchés publics de 2016 s'apparente très nettement à notre article L. 2512-3 :

« […] § 2 La présente loi ne s'applique pas aux marchés publics qui ne sont pas par ailleurs exclus en vertu du paragraphe 1er [relevant de la défense et de la sécurité] dans la mesure où la protection des intérêts essentiels de la sécurité du Royaume ne peut être garantie par des mesures moins intrusives, par exemple en imposant des conditions en vue de protéger la confidentialité des informations que le pouvoir adjudicateur met à disposition dans le cadre d'une procédure de passation prévue par la présente loi.

En outre, et en conformité avec l'article 346, paragraphe 1er, a), du Traité sur le fonctionnement de l'Union européenne, la présente loi ne s'applique pas aux marchés publics qui ne sont pas par ailleurs exclus en vertu du paragraphe 1er du présent article, dans la mesure où l'application de la présente loi obligerait le Royaume à fournir des informations dont il estimerait la divulgation contraire aux intérêts essentiels de sa sécurité.

§ 3. Lorsque la passation et l'exécution du marché public sont déclarés secrets ou doivent s'accompagner de mesures particulières de sécurité, conformément aux dispositions législatives, réglementaires ou administratives en vigueur dans le Royaume, la présente loi ne s'applique pas, pour autant qu'il est établi que la protection des intérêts essentiels concernés ne peut être garantie par des mesures moins intrusives, telles que celles visées au paragraphe 2, alinéa 1er. »

Sans avoir réservé un sort particulier à ses OIV (puisqu'un tel régime n'existe pas encore en Belgique), le Gouvernement belge a cependant édicté une circulaire[128], le 11 septembre 2023, qui incite les pouvoirs adjudicateurs fédéraux à respecter et utiliser comme cadre d'interprétation une « boîte à outils » visant à réduire les risques de sécurité dans le cadre des marchés publics et procéder à un « quick scan » pour tous les marchés publics susceptibles d'avoir un impact sur la sécurité nationale.

[128] https://bosa.belgium.be/sites/default/files/content/documents/2023_10_25_publicatie_BS.pdf.

Ladite circulaire invite à faire un plein usage des dispositions permettant de protéger les intérêts essentiels de l'Etat, après avoir réalisé un examen de proportionnalité à l'aune de la jurisprudence de la CJUE.

On notera aussi que la République Tchèque a invoqué le bénéfice de cette exception pour le projet de centrale nucléaire de Dukovany.

2. NECESSITE DE LEGIFERER ET OBJECTIFS POURSUIVIS

2.1. NECESSITE DE LEGIFERER

La présente disposition précise le champ d'application des règles définies au titre II du livre V de la deuxième partie et au titre II du livre II de la troisième partie du code de la commande publique du code de la commande publique, ce qui exige l'intervention du législateur.

Il apparaît nécessaire de légiférer pour renforcer, en tenant compte de la marge d'appréciation permise par le droit de l'Union, la protection des intérêts essentiels de la Nation à l'occasion des contrats de la commande publique les plus sensibles des OIV.

La mesure restreint la liberté d'accès à la commande publique et relève donc de la loi.

2.2. OBJECTIFS POURSUIVIS

La mesure vise à clarifier l'état du droit afin de tenir compte du dernier état de la jurisprudence européenne et à définir les marchés et contrat de concessions des OIV qui sont exclus des règles de la commande publique afin de prévenir tout risque d'ingérence ou d'atteinte à la continuité de leurs activités d'importance vitale.

3. OPTIONS ENVISAGEES ET DISPOSITIF RETENU

3.1. OPTIONS ENVISAGEES

Le code de la commande publique permet déjà aujourd'hui, tout particulièrement à ses articles L. 2512-3 et L. 3212-3, d'écarter son application sur le fondement de la protection des intérêts essentiels de l'État.

L'option de ne pas légiférer a cependant été écartée parce qu'il importe que l'État définisse lui-même ce qui apparaît essentiel à la protection des intérêts fondamentaux de la Nation et le niveau de protection à atteindre.

Une mise en concurrence à des conditions définies par l'acheteur permettant la consultation d'opérateurs fiables demeurera toutefois possible dans la mesure compatible avec la protection de nos intérêts essentiels.

L'option d'exclure du droit commun l'ensemble des contrats de la commande publique des OIV qui y sont soumis a été écartée afin de garantir la conformité de la mesure au droit de l'Union (et éviter qu'elle soit utilisée pour des marchés ou contrats de concessions dépourvus de tout lien avec la protection des intérêts essentiels de l'État, par exemple ceux portant sur des fournitures usuelles sans spécificité ni contribution à la sécurité, ou non nécessaires pour la continuité des activités d'importance vitale).

3.2. DISPOSITIF RETENU

L'option retenue consiste à adopter une disposition spécifique, proche de celle retenue dans le cadre de la loi n° 2024-450 du 21 mai 2024 relative à l'organisation de la gouvernance de la sûreté nucléaire et de la radioprotection pour répondre au défi de la relance de la filière nucléaire, qui ne serait pas codifiée dans le code de la commande publique, compte tenu de sa circonscription aux seuls OIV soumis au code de la commande publique.

Elle prévoit l'application du titre II du livre V de la deuxième partie de la commande publique (pour les marchés) et du titre II du livre II de la troisième partie du code de la commande publique (pour les contrats de concession), qui correspondent aux régimes des contrats qui étaient exclus du champ d'application du code des marchés publics et de l'ordonnance n° 2016-65 du 29 janvier 2016 relative aux contrats de concession dans l'état du droit antérieur à la codification du droit de la commande publique.

Elle s'appliquera aux marchés publics et contrats de concessions relatifs à la conception, la qualification, la fabrication, la modification, la maintenance ou le retrait des structures, équipements, systèmes, matériels, composants ou logiciels nécessaires à la protection des infrastructures critiques ou à l'exercice de l'activité d'importance vitale de l'opérateur, à la condition que cette protection ou cet exercice ne puisse être garanti par d'autres moyens.

Afin de garantir que ces dérogations soient bien conformes au droit de l'Union européenne et ne risquent pas d'être utilisés pour des contrats dépourvus de tout lien avec la protection des intérêts essentiels de l'État, les OIV devront informer l'autorité administrative qu'ils mettent en œuvre cette mesure. De la sorte, il serait explicite que les acheteurs publics et entités adjudicatrices devraient être en mesure d'établir qu'il n'est pas possible de prévenir ces risques par des mesures de moindre effet (par exemple en appliquant l'article L. 2132-1, alinéa 3 du code qui permet à l'acheteur d'« imposer aux opérateurs économiques des exigences visant à protéger la confidentialité des informations qu'il communique dans le cadre de la procédure de passation d'un marché » ou en imposant l'utilisation de certains

équipements critiques pour des raisons techniques ou juridiques). Les conditions et délais d'informations seront précisés par voie réglementaire.

4. ANALYSE DES IMPACTS DES DISPOSITIONS ENVISAGEES

4.1. IMPACTS JURIDIQUES

4.1.1. Impacts sur l'ordre juridique interne

Comme exposé *supra*, la constitutionnalité des dispositions envisagées ne fait pas débat. Elles prévoient en effet des dérogations aux principes de la commande publique à raison de l'objet du marché ou du contrat de concession quand le respect des procédures de droit commun est de nature à compromettre la continuité d'une activité d'importance vitale, laquelle est sans conteste un motif d'intérêt général.

Des articles L. 1332-20 à L. 1332-22 sont créés dans le code de la défense au sein du Chapitre II « Résilience des activités d'importance vitale », section 4 « Marchés publics et contrats de concessions relatifs à la sécurité des activités d'importance vitale ».

La mesure ne nécessite aucune abrogation. Elle n'a pas vocation à être codifiée dans le code de la commande publique.

4.1.2. Articulation avec le droit international et le droit de l'Union européenne

Des directives européennes en matière de commande publique ont été publiées en 2014. Il s'agit :

- de la directive 2014/23/UE du 26 février 2014 sur l'attribution de contrats de concession ;
- de directive 2014/24/UE du 26 février 2014 sur la passation des marchés publics ;
- de la directive 2014/25/UE 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.

Par ailleurs, l'ensemble des règles régissant tous les contrats constituant des marchés de défense ou de sécurité sont encadrés par la directive 2009/81/CE, qui harmonise les règles de passation des marchés de défense ou de sécurité à l'échelle de l'Union.

En particulier, les articles 15 de la directive 2014/24 et 24 de la directive 2014/25 prévoient une exclusion de leur application pour des raisons de sécurité, notamment « dans la mesure où la protection des intérêts essentiels de la sécurité d'un État membre ne peut être garantie par des mesures moins intrusives ».

Les dispositions envisagées s'inscrivent pleinement dans ce cadre normatif européen ; il ne se heurte à aucun obstacle d'ordre conventionnel, dès lors que les marchés publics et contrats de concessions mentionnés par le projet de loi, dont l'objet est précisément défini, peuvent être considérés comme hors du champ de la directive au titre de la protection des intérêts essentiels de l'Etat, à plus forte raison dans la mesure où le projet rappelle que la protection de ces intérêts ne doit pas, en l'espèce, pouvoir être garantie par des mesures moins intrusives.

4.2. IMPACTS ECONOMIQUES ET FINANCIERS

4.2.1. Impacts macroéconomiques

La mesure n'a, par elle-même, aucune incidence macroéconomique. Elle aura néanmoins une contribution indirecte au titre de l'amélioration de la défense économique de la Nation, notamment concernant la sécurité d'approvisionnement.

4.2.2. Impacts sur les entreprises

Comme exposé *supra*, l'adoption des dispositions envisagées permettrait aux OIV soumis au code de la commande publique de faire valoir leur statut lorsqu'ils passent certaines marchés publics ou contrats de concession, pour pouvoir déroger à certaines dispositions du code de la commande publique, et ainsi écarter les candidats problématiques.

La mesure n'a, par elle-même, aucune incidence générale sur les entreprises. Elle pourra entraîner dans certains cas des restrictions à la liberté d'accès à la commande publique, justifiées par la protection des intérêts essentiels de la Nation et limitées par le maintien du principe d'une mise en concurrence et la nécessité de tenir compte de la pluralité d'offres susceptibles de répondre au besoin.

4.2.3. Impacts budgétaires

Sans objet.

4.3. IMPACTS SUR LES COLLECTIVITES TERRITORIALES

Le cas échéant, les collectivités désignées par l'autorité administrative en tant qu'opérateurs d'importance vitale sont soumises aux dispositions de commande publique visées par le présent projet de loi.

4.4. IMPACTS SUR LES SERVICES ADMINISTRATIFS

Les services administratifs verront *de facto* leur mission de supervision évoluer puisqu'ils devront contrôler le respect effectif des dispositions spéciales de commande publique appliquées aux OIV publics.

En outre, l'autorité administrative est informée par les entités adjudicatrices et les pouvoirs adjudicateurs lorsque ces derniers ont recours aux règles prévues par le présent article, selon des modalités renvoyées à un décret.

4.5. IMPACTS SOCIAUX

4.5.1. Impacts sur la société

La présente mesure contribuera à l'amélioration de la défense économique de la Nation.

4.5.2. Impacts sur les personnes en situation en handicap

Sans objet.

4.5.3. Impacts sur l'égalité entre les femmes et les hommes

Sans objet.

4.5.4. Impacts sur la jeunesse

Sans objet.

4.5.5. Impacts sur les professions réglementées

Sans objet.

4.6. IMPACTS SUR LES PARTICULIERS

Sans objet.

4.7. IMPACTS ENVIRONNEMENTAUX

La mesure n'a, par elle-même, aucun impact environnemental. Elle aura néanmoins une contribution indirecte au titre de l'amélioration de la défense économique de la Nation, notamment concernant la protection contre les actes de malveillance sur point d'importance vitale et donc sur la réduction associée des risques pour l'environnement.

5. CONSULTATIONS MENEES ET MODALITES D'APPLICATION

5.1. CONSULTATIONS MENEES

Une concertation de l'ensemble des ministères coordonnateurs a été réalisée sur cette mesure.

En application de l'article L. 1212-2 du code général des collectivités territoriales, les présentes dispositions ont été soumises à l'examen du Conseil national d'évaluation des normes qui a rendu un avis défavorable le 22 mai 2024.

Enfin, le service national des enquêtes administratives de sécurité, le coordinateur général de la sécurité nucléaire, le service juridique du Secrétariat général des affaires européennes et l'Agence nationale de sécurité des systèmes d'informations ont également été consultés.

5.2. MODALITES D'APPLICATION

5.2.1. Application dans le temps

Les présentes dispositions entreront en vigueur le lendemain de la publication de la présente loi au *Journal officiel* de la République française. Toutefois, afin de produire des effets, elles nécessiteront l'adoption d'un décret en Conseil d'Etat (mentionné *infra, 5.2.3.*).

5.2.2. Application dans l'espace

Conformément aux dispositions de l'article L. 1 du code de la défense, s'agissant d'une mesure liée à la politique de sécurité nationale ou à la politique de défense, les présentes dispositions s'appliqueront de plein droit sur l'ensemble du territoire de la République, sans qu'aucune mention expresse d'application ne soit requise pour les collectivités d'outre-mer.

5.2.3. Textes d'application

Les présentes dispositions feront l'objet d'un décret en Conseil d'Etat.

TITRE II – CYBERSECURITE

CHAPITRE IER – DE L'AUTORITE NATIONALE DE SECURITE DES SYSTEMES D'INFORMATION

Article 5 – Missions et compétences de l'autorité nationale

1. ÉTAT DES LIEUX

1.1. CADRE GENERAL

Dans son panorama de la menace de 2023[129], l'Agence nationale de la sécurité des systèmes d'information (ANSSI) a identifié quatre tendances principales en matière cyber. L'espionnage stratégique et industriel est la menace qui a le plus mobilisé ses équipes. Les cyberattaques à des fins d'extorsion se sont maintenues à un niveau élevé. L'augmentation de 30% du nombre d'attaques par rançongiciel portées à la connaissance de l'ANSSI peut en témoigner. L'ANSSI a également constaté un regain du nombre d'attaques à des fins de promotion de discours politique ou de déstabilisation. Enfin, il est établi que l'exploitation de vulnérabilités « jour-zéro »[130] et « jour-un »[131] reste une porte d'entrée de choix pour les attaquants.

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

Aux termes de l'article R. 2321-1 du même code : « L'autorité nationale de sécurité des systèmes d'information mentionnée à l'article L. 2321-1 est l'Agence nationale de la sécurité des systèmes d'information ».

---

[129] ANSSI, « Panorama de la menace informatique 2023 », février 2024.

[130] Aussi appelée « zero-day », il s'agit d'une vulnérabilité n'ayant fait l'objet d'aucune publication ni correctif de sécurité au moment de son exploitation.

[131] Aussi appelée « one-day » ou « n-day », il s'agit d'une vulnérabilité pour laquelle un correctif de sécurité est disponible, mais n'a pas été déployé par l'utilisateur, rendant l'exploitation de la vulnérabilité possible.

Créée par le décret n° 2009-834 du 7 juillet 2009 modifié par le décret n° 2020-455 du 21 avril 2020, l'ANSSI, service à compétence nationale rattaché au secrétaire général de la défense et de la sécurité nationale (SGDSN), est l'autorité nationale de sécurité des systèmes d'information. En cette qualité, l'ANSSI « propose 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 elle coordonne, dans le cadre des orientations fixées par le Premier ministre, l'action gouvernementale en matière de défense des systèmes d'information ». Par ailleurs, le ministre de la défense dispose de compétences spécifiques en matière de cybersécurité prévues par la sous-section 4 de la section 2 du chapitre I[er] du titre I[er] du livre IV du code de la défense.

1.2. CADRE CONSTITUTIONNEL

Aux termes de l'article 88-1 de la Constitution : « La République participe aux Communautés européennes et à l'Union européenne, constituées d'Etats qui ont choisi librement, en vertu des traités qui les ont instituées, d'exercer en commun certaines de leurs compétences ». Le Conseil constitutionnel déduit de cette disposition que « la transposition en droit interne d'une directive communautaire résulte d'une exigence constitutionnelle »[132].

De ce fait, le Conseil constitutionnel juge qu'il lui appartient de veiller au respect de cette exigence lorsqu'il est saisi dans les conditions prévues par l'article 61 de la Constitution d'une loi ayant pour objet de transposer en droit interne une directive de l'Union européenne[133], même si son contrôle est limité.

Il en va de même pour une loi ayant pour objet d'adapter le droit interne à un règlement de l'Union européenne[134].

1.3. CADRE CONVENTIONNEL

Le présent article vise à transposer les mesures issues de l'article 8 de la directive 2022/2555[135], ci-après « NIS 2 », en ce qui concerne la désignation de l'autorité nationale de

---

[132] Voir notamment la décision n° 2004-496 DC du 10 juin 2004, « Loi pour la confiance dans l'économie numérique ».

[133] Voir la décision n° 2006-543 DC du 30 novembre 2006 « Loi relative au secteur de l'énergie », considérants 4 à 7.

[134] Voir par exemple la décision n° 2018-765, « Loi relative à la protection des données personnelles », considérant 3.

[135] 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).

sécurité des systèmes d'information et sa compétence pour contrôler la mise en œuvre de la directive. Il ouvre le titre II dont le principal objet est de transposer l'intégralité de la directive NIS 2.

La directive NIS 2 remplace 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 directive NIS1), laquelle a été transposée en France par 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.

Afin de prendre en compte l'évolution de la menace cyber devenue systémique, la directive NIS 2 a considérablement élargi le périmètre initial des acteurs et secteurs régulés par NIS 1 qui ciblait uniquement les acteurs et opérateurs les plus stratégiques via la mise en place d'une procédure national d'identification. En France, cet élargissement du périmètre se traduit par une augmentation estimée du nombre d'entités régulées de 500 à près de 15 000, et une augmentation du nombre de secteurs régulés de 6 à 18. La directive NIS2 élargit également le périmètre des systèmes d'information à sécuriser. Alors que la directive NIS1 prévoyait une identification des systèmes d'information essentiels sur lesquels les obligations de la directive porteraient, la directive NIS2 s'applique par défaut à l'ensemble des systèmes d'information de l'entité. Des mécanismes d'exemption de certains systèmes d'information sont toutefois permis si ces derniers n'impactent pas la réalisation des activités ou la fourniture des services de l'entité.

La directive NIS 2 consacre enfin le principe de proportionnalité en prévoyant deux niveaux d'entités régulées, les entités importantes et essentielles, classées selon leur degré de criticité, leur taille et leur chiffre d'affaires (pour les entreprises), afin d'adapter le niveau d'exigence. Les entités importantes, qui représentent la plus grande proportion des acteurs concernés par le projet de loi, se verront imposer des exigences de sécurité de base (de l'ordre de « l'hygiène numérique »), pour diminuer leur probabilité d'être atteintes par un rançongiciel courant. Les entités essentielles sont des structures déjà sensibilisées ou confrontées à la menace cyber. Elles seront en partie des opérateurs déjà régulés, et donc déjà soumises depuis des années à la réglementation NIS et/ou au dispositif de sécurité des activités d'importance vitale (SAIV).

Au sens de la directive NIS 2, l'autorité nationale de sécurité des systèmes d'information est l'autorité compétente pour contrôler la mise en œuvre de la directive en France. Elle est également le point de contact unique, pour les autorités compétentes des autres États membres, pour la Commission et l'Agence de l'Union européenne pour la cybersécurité (ENISA), ainsi que pour les autres autorités sectorielles compétentes sur ces sujets. Elle est également centre national de réponse aux incidents de sécurité informatique (CSIRT national), autorité chargée de la gestion des incidents de cybersécurité et crises cyber ainsi que représentante de la France dans le cadre de la coopération internationale organisée par la directive NIS 2, notamment au sein de EU-CyCLONe (article 16 de la directive NIS 2) et au sein du réseau des CSIRT (article 15 de la directive NIS 2).

1.4. ÉLEMENTS DE DROIT COMPARE

La Belgique, qui est aujourd'hui l'un des rares Etats membres à avoir finalisé la transposition de la directive NIS 2 dans son droit national, a fait le choix, dans son projet de loi, de désigner une autorité nationale de cybersécurité unique, le Centre pour la Cybersécurité Belgique, qui n'est pas explicitement cité dans la loi afin de respecter l'indépendance du pouvoir exécutif, mais sera désigné par lui. Le texte prévoit la possibilité de nommer des autorités sectorielles ainsi que des services d'inspection sectoriels.

La Belgique a également fait le choix d'inscrire dans son projet de loi le rôle de l'autorité nationale de cybersécurité afin de centraliser ses compétences, que ce soit celles prévues par la directive NIS 2 ou celles déjà dévolues au Centre pour la Cybersécurité Belgique. En cohérence avec la directive, le texte liste les missions prévues par NIS 2 (voir *supra*) ainsi que celles mentionnées en tant qu'autorité nationale, dont la gestion, par une approche intégrée et centralisée, des différents projets relatifs à la cybersécurité et la coordination entre autorités publiques et le secteur privé ou le monde scientifique, en matière de gestion des crises cyber et en tant que centre de réponse à incident national.

2. NECESSITE DE LEGIFERER ET OBJECTIFS POURSUIVIS

2.1. NECESSITE DE LEGIFERER

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

Toutefois, le rôle de l'autorité nationale de sécurité des systèmes d'information en matière de sécurité des systèmes d'information n'est défini que par des dispositions isolées[136]. Aussi importe-t-il de disposer que l'autorité nationale de sécurité des systèmes d'information est chargée de la mise en œuvre de la politique du gouvernement en matière de sécurité des systèmes d'information et de son contrôle.

Il convient de noter qu'outre le non-respect d'une exigence constitutionnelle (cf. paragraphe 1.2), la non transposition, le retard dans la transposition, l'absence de communication des mesures de transposition ou la mauvaise transposition d'une directive européenne peuvent

[136] Article L. 33-1, L. 33-14 et L. 102 du code des postes et des communications électroniques ; Article L. 631-1 du code monétaire et financier.

entraîner un risque contentieux pour la France. En effet, au niveau de l'Union européenne, la France est susceptible de faire l'objet d'une procédure de manquement devant la Cour de justice de l'Union européenne, dans la majorité des cas à l'initiative de la Commission européenne, impliquant des sanctions pécuniaires (somme forfaitaire ou astreinte).

Par ailleurs, en droit interne, le juge administratif peut être conduit à sanctionner un défaut de transposition de deux manières :

1. par une annulation du texte de transposition qui se révèlerait infidèle ou incomplet ;
2. par l'annulation de procédures ou actes conformes au droit interne mais ne répondant pas aux objectifs fixés par des dispositions non transposées de directives ou en contradiction avec des dispositions précises et inconditionnelles qu'elles contiennent.

Les missions de l'autorité nationale de sécurité des systèmes d'information sont duales (sécurité des systèmes d'information et défense des systèmes d'information). En effet, l'autorité nationale de sécurité des systèmes d'information est aussi investie de compétences qui, si elles ne relèvent pas strictement du champ de la sécurité nationale ou de la défense, concourent pour partie à la stratégie de sécurité nationale ainsi qu'à la défense et à la promotion des intérêts fondamentaux de la Nation. A titre d'exemple, la qualification et la certification de produits et de prestataires de services de confiance dans le cadre des obligations des opérateurs d'importance vitale ou la délivrance d'agréments à des produits de sécurité. Si les missions de l'autorité nationale de défense des systèmes d'information sont clairement définies dans la loi, celles de l'autorité nationale de sécurité des systèmes d'information ne sont quant à elles définies par aucun texte, si ce n'est par des dispositions isolées. La dualité de ses missions implique, d'ailleurs, que ces compétences ne peuvent pas figurer au sein de code de la défense, à l'instar d'autres services de l'Etat (cf. *infra*).

Par ailleurs, si l'organisation et la répartition des compétences entre les services de l'Etat relève, en principe, du domaine règlementaire, l'organisation administrative liée à l'exercice de certaines compétences peut, toutefois, figurer au niveau de la loi. A titre d'exemples, le code de la sécurité intérieure prévoit dans son livre Ier, un titre II portant sur l'organisation administrative qui aborde notamment le rôle des préfets en tant que représentant de l'Etat. Le même code détermine à l'article L. 811-2 les compétences des services spécialisés de renseignement au titre de la politique publique de renseignement. L'autorité nationale de sécurité des systèmes d'information mettant en œuvre la politique du gouvernement en matière de sécurité des systèmes d'information, sa compétence doit donc être déterminée au niveau de la loi pour en prévoir le rôle prépondérant au regard d'autres services dont les missions figurent dans la loi.

De plus, cette désignation de l'autorité nationale de sécurité des systèmes d'information comme autorité compétente chargée de la cybersécurité au sens de l'article 8 de la directive a des implications fortes pour les collectivités territoriales et pour les entreprises, compte tenu

notamment de la mise en place d'un pouvoir de supervision et de contrôle. Ces éléments justifient que cette mission soit inscrite dans la loi.

2.2. OBJECTIFS POURSUIVIS

Dans un contexte d'augmentation du volume de cyberattaques auquel la France fait face[137], et de leur sophistication croissante, disposer d'une autorité nationale cheffe de file identifiée comme assurant la coordination, à l'échelon national, de l'action gouvernementale et des différents services en matière de cybersécurité, constitue un atout essentiel pour doter la France d'une cyber résilience de tout premier ordre, objectif fixé par le Président de la République dans la revue nationale stratégique de 2022.

Dans cette perspective, le présent article permet de transposer l'article 8 de la directive NIS2 en prévoyant l'existence d'une autorité nationale de sécurité des systèmes d'information chargée de la mise en œuvre de la législation et de la politique du Gouvernement en matière de sécurité des systèmes d'information, dont les missions et leurs conditions d'exercice seront précisées par décret.

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

3. OPTIONS ENVISAGEES ET DISPOSITIF RETENU

3.1. OPTIONS ENVISAGEES

Deux options pouvaient être envisagées : codifier l'article dans le code de la défense ou prévoir les missions dans une loi autonome, hors du code de la défense.

3.2. OPTION RETENUE

Le choix de désigner dans la loi une autorité nationale cheffe de file identifiée comme assurant la coordination, à l'échelon national, de l'action gouvernementale et des différents services en matière de cybersécurité, lui permet de disposer des compétences nécessaires pour bâtir et organiser la protection de la Nation face aux cyberattaques et ainsi renforcer le niveau

[137] Dans son « Panorama de la menace informatique 2023 » publié en février 2024, l'ANSSI a observé une augmentation de 30% du nombre d'attaques par rançongiciel portées à sa connaissance en 2023 par rapport à la même période en 2022.

de cybersécurité global et la stabilité du cyberespace, en coordination étroite avec l'ensemble des acteurs de l'État disposant de compétences en matière de cybersécurité et de cyberdéfense.

En outre, l'option de retenir la loi autonome trouve sa justification dans les éléments suivants.

Les missions de l'autorité nationale de sécurité des systèmes d'information sont duales puisqu'elles relèvent à la fois de la sécurité des systèmes d'information et de la défense des systèmes d'information telle que définie par l'article L. 2321-1 du code de la défense. L'article 5, en ce qu'il porte le rôle de mise en œuvre de la politique du gouvernement en matière de sécurité des systèmes d'information, se justifie puisque certaines de ses missions, qui seront précisées par décret en Conseil d'Etat, ne relèvent pas strictement du champ de la sécurité nationale ou de la défense. Par exemple, ce sont les cas de la qualification et de la certification de produits et de prestataires de services de confiance ou de la délivrance d'agréments à des produits de sécurité ou des services de confiance en vertu de règlements européens tels que le règlement eIDAS ou le règlement CSA qui ont trait au développement de la confiance numérique sur le marché intérieur.

En effet, si le code de la défense intègre des dispositions plus larges que la défense militaire stricto sensu, elles ont systématiquement trait à l'organisation générale de la défense et de la sécurité nationale, qu'il s'agisse de l'organisation des services de l'Etat et des établissements qui lui sont rattachés ou des règles applicables à des entités dont l'atteinte risquerait d'affecter la vie de la Nation, notamment la protection de la population, l'intégrité du territoire et la permanence des institutions de la République (régimes d'exceptions, défense économique, etc.).

De manière générale, l'article L. 1111-1 du code de la défense précise que « *L'ensemble des politiques publiques concourt à la sécurité nationale* ». Pour autant, l'ensemble des règles permettant de mettre en œuvre ces politiques publiques ne figurent pas au sein du code de la défense. Il en va ainsi de la sécurité des systèmes d'information dont certaines dispositions figurent également dans d'autres textes codifiés ou non (le code monétaire et financier par exemple au sujet de la vérification de l'identité).

Les notions de cybersécurité et de cyberdéfense présentent ce lien d'interdépendance sans qu'elles ne recouvrent des périmètres identiques. Ainsi, la cyberdéfense est l'« *Ensemble des moyens mis en place par un État pour défendre dans le cyberespace les systèmes d'information jugés d'importance vitale, qui contribuent à assurer la cybersécurité* » tandis que la cybersécurité est définie comme un « « *État d'un système d'information qui résiste aux cyberattaques et aux pannes accidentelles survenant dans le cyberespace* » [138]. La cyberdéfense met notamment en œuvre la lutte informatique défensive, définie comme un «

[138] Cf. JORF n° 0219 du 19 septembre 2017.

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

En outre, l'article L. 2321-1 du code de la défense dispose expressément que « *Dans le cadre de la stratégie de sécurité nationale et de la politique de défense, le Premier ministre définit la politique et coordonne l'action gouvernementale en matière de sécurité et de défense des systèmes d'information. Il dispose à cette fin de l'autorité nationale de sécurité des systèmes d'information qui assure la fonction d'autorité nationale de défense des systèmes d'information* ». Or, les missions qui relèvent traditionnellement du développement de l'écosystème de la cybersécurité telles que la certification ou la qualification de produits ou de prestataires de services de confiance ont été confiées directement à l'autorité nationale. A ce titre, c'est le directeur général de l'ANSSI qui délivre ces décisions administratives individuelles à titre de compétences propres au titre de l'article 4 du décret n° 2009-834 et non par délégation de signature du Premier ministre.

Partant, la disparition de l'article 5, par le rattachement des missions de l'autorité nationale de sécurité des systèmes d'information à l'article L. 2321-1 du code de la défense pour l'ensemble des missions qui relèvent de la certification et de la qualification, liées à la mise en œuvre de règlement européens ou d'exigences nationale, ne serait pas conforme à la portée de cet article du code de la défense qui ne s'inscrit que par le prisme de la stratégie de sécurité nationale et de la politique de défense et de fait, de la compétence du Premier ministre.

A titre d'illustration, l'ordonnance n° 2005-1516 (dont une partie a vocation à disparaître avec la simplification portée par le projet de loi), qui est le fondement de niveau législatif des exigences du référentiel général de sécurité, n'a jamais conduit à codifier les missions qui en découlent au sein du code de la défense. Pas plus, par ailleurs, que la loi n° 2018-133 précitée transposant la directive NIS 1 qui s'adressait aux opérateurs de services essentiels ainsi qu'aux fournisseurs de services numériques qui est restée une loi autonome et n'a pas fait l'objet de codification au sein du code de la défense.

4. ANALYSE DES IMPACTS DES DISPOSITIONS ENVISAGEES

4.1. IMPACTS JURIDIQUES

4.1.1. Impacts sur l'ordre juridique interne

La déclinaison, au niveau règlementaire, des missions de l'autorité nationale modifiera :

- le décret n° 2009-834 précité ;
- le décret n° 2002-535 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information ;
- le décret n° 2010-112 pris pour l'application des articles 9, 10 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 ;
- le décret n° 2015-350 relatif à la qualification des produits de sécurité et des prestataires de service de confiance pour les besoins de la sécurité des systèmes d'information ;
- le décret n° 97-34 relatif à la déconcentration des décisions administratives individuelles le cas échéant.

En outre, des dispositions réglementaires prévoiront que certains ministres, en particulier le ministre chargé de la défense, exerceront les missions de l'autorité nationale de sécurité des systèmes d'information, pour son compte ou dans les domaines relevant spécifiquement de leurs attributions.

4.1.2. Articulation avec le droit international et le droit de l'Union européenne

La mesure prévue à l'article 5 vise à transposer l'article 8 de la directive NIS 2.

4.2. IMPACTS ECONOMIQUES ET FINANCIERS

4.2.1. Impacts macroéconomiques

Face à une menace qui se massifie, des acteurs malveillants qui se professionnalisent et la multiplication des attaques, tous les secteurs et toutes les tailles d'entreprise et d'organisation sont touchés. Cette augmentation constante des attaques[139] coûte par ailleurs très cher aux entreprises, aux administrations et aux particuliers. Le coût direct d'une cyberattaque peut par exemple s'élever à environ un million d'euros pour une collectivité territoriale, voire à plus de cinq millions d'euros pour un centre hospitalier.

De manière générale, désigner dans les textes l'autorité nationale et clarifier son rôle permettra de lutter plus efficacement contre des incidents de cybersécurité qui peuvent nuire à

[139] Dans son « Panorama de la menace informatique 2023 » publié en février 2024, l'ANSSI a observé une augmentation de 30% du nombre d'attaques par rançongiciel portées à sa connaissance en 2023 par rapport à la même période en 2022.

la poursuite des activités économiques sur le marché intérieur, entraîner des pertes financières, entamer la confiance des utilisateurs et causer un préjudice majeur à l'économie et la société. Des impacts plus directs, notamment ceux liés à la mise en œuvre de la directive, sont mentionnés dans la suite de l'étude d'impact, en particulier dans les chapitres II relatif à la cyber résilience et III pour ce qui concerne le régime de supervision.

4.2.2. Impacts sur les entreprises

En facilitant la gestion de crise d'origine cyber avec les partenaires européens ou relevant du secteur privé, il est attendu que les impacts intersectoriels et transfrontaliers de ces crises soient mieux anticipés et formalisés, permettant d'identifier de meilleures mesures de remédiation et donc de réduire plus rapidement les impacts métiers associés et le coût des crises pour les organisations.

L'ancrage du rôle de l'autorité nationale dans la loi aura aussi pour effet de renforcer la lutte proactive contre les cyberattaques. En effet, les qualifications, certifications, agréments et labels permettent d'accélérer la diffusion de produits et services numériques de confiance avec un impact positif sur l'économie, *via* le développement de cet écosystème et *via* le renforcement de la cybersécurité des organisations utilisatrices et donc de leur compétitivité.

4.2.3. Impacts budgétaires

L'inscription, au niveau règlementaire, du rôle de centre national de réponse aux incidents informatiques renforcera les capacités de supervision de l'ANSSI, sans engendrer en tant que telle d'impact sur ses moyens (qui devront en revanche être adaptés à l'extension de son champ de compétence découlant des autres dispositions du projet de loi).

La mise en œuvre des responsabilités du ministre de la défense sur son périmètre de responsabilité n'engendrera pas non plus de coût supplémentaire, dès lors qu'il met déjà en œuvre des responsabilités similaires.

4.3. IMPACTS SUR LES COLLECTIVITES TERRITORIALES

Sans objet.

4.4. IMPACTS SUR LES SERVICES ADMINISTRATIFS

Cf. §4.2.3 Impacts budgétaires.

4.5. IMPACTS SOCIAUX

4.5.1. Impacts sur la société

Sans objet.

4.5.2. Impacts sur les personnes en situation de handicap

Sans objet.

4.5.3. Impacts sur l'égalité entre les femmes et les hommes

Sans objet.

4.5.4. Impacts sur la jeunesse

Sans objet.

4.5.5. Impacts sur les professions réglementées

Sans objet.

4.6. IMPACTS SUR LES PARTICULIERS

Sans objet.

4.7. IMPACTS ENVIRONNEMENTAUX

Sans objet.

5. CONSULTATIONS ET MODALITES D'APPLICATION

5.1. CONSULTATIONS MENEES

Conformément aux dispositions de l'article L. 1212-2 du code général des collectivités territoriales, la présente disposition a été soumise à l'examen du Conseil national d'évaluation des normes (CNEN) qui a rendu un avis défavorable le 22 mai 2024.

Sur le fondement de l'article 8 de la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, la Commission nationale de l'informatique et des libertés (CNIL) a été consultée à titre facultatif. Elle a rendu un avis favorable le 23 mai 2024

au renforcement des mesures en matière de cybersécurité, appelant toutefois à s'assurer de la cohérence des exigences de sécurité découlant des principes relatifs à la protection des données avec celles issues de la directive NIS 2 ainsi qu'à une coordination entre la CNIL et l'ANSSI sur la mise en œuvre de NIS 2.

5.2. MODALITES D'APPLICATION

5.2.1. Application dans le temps

Le présent article entrera en vigueur le lendemain de la publication de la loi au *Journal officiel* de la République française.

5.2.2. Application dans l'espace

Conformément à l'article 40 du présent projet de loi, le titre II est applicable dans les îles Wallis et Futuna, en Polynésie française, en Nouvelle-Calédonie et dans les Terres australes et antarctiques françaises, sous réserve des adaptations suivantes :

1° 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 applicables localement.

2° Dans les îles Wallis et Futuna, en Polynésie française et en Nouvelle-Calédonie, les sanctions pécuniaires encourues en vertu du titre II de la présente loi sont prononcées en monnaie locale, compte tenu de la contre-valeur de l'euro dans cette monnaie.

Pour l'application du titre II à Saint-Barthélemy, Saint-Pierre-et-Miquelon, dans les îles Wallis et Futuna, en Polynésie française, en Nouvelle-Calédonie et dans les Terres australes et antarctiques françaises, les références à la directive (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 et aux règlements de l'Union européenne sont remplacées par la référence aux règles en vigueur en métropole en vertu de la même directive et des mêmes règlements.

5.2.3. Textes d'application

Un décret en Conseil d'Etat précisera les missions de l'autorité nationale de sécurité des systèmes d'information ainsi que celles des organismes désignés par le Premier ministre pour exercer, dans le domaine de la défense, les missions de cette autorité. Il prévoira le cas échéant, les modalités de leur coopération avec l'Agence nationale de sécurité des systèmes d'information.

CHAPITRE II – DE LA CYBER RESILIENCE

Article 6 – Définitions

1. ETAT DES LIEUX

1.1. CADRE GENERAL

Le droit national, que ce soit au niveau législatif ou réglementaire, ne comporte pas d'appareil de définitions des notions et des concepts liés à la cybersécurité tels que « bureau d'enregistrement », « prestataire de service de confiance », prestataire de service de confiance qualifié », « office d'enregistrement » ou encore « service de centre de données ».

L'existant est dispersé, lacunaire ou bien encore cantonné à un niveau infra-réglementaire. Par exemple, la seule notion de système d'information est définie par l'article 4 de la directive NIS 1, par 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 le décret n° 2019-1088 relatif au système d'information et de communication de l'Etat et à la direction interministérielle du numérique et par l'instruction générale interministérielle 1300 sur la protection du secret de la défense nationale.

1.2. CADRE CONSTITUTIONNEL

Aux termes de l'article 88-1 de la Constitution : « La République participe aux Communautés européennes et à l'Union européenne, constituées d'Etats qui ont choisi librement, en vertu des traités qui les ont instituées, d'exercer en commun certaines de leurs compétences ». Le Conseil constitutionnel déduit de cette disposition que « la transposition en droit interne d'une directive communautaire résulte d'une exigence constitutionnelle »[140]. Si les règlements eIDAS et CSA sont directement applicables, la directive NIS 2 contient de nombreuses définitions dont certaines renvoient également à celles du règlement.

[140] Voir notamment la décision n° 2004-496 DC du 10 juin 2004, « Loi pour la confiance dans l'économie numérique ».

Tant la transposition que le principe de clarté de la loi et l'objectif de valeur constitutionnelle d'intelligibilité et d'accessibilité de la loi imposent d'adopter des dispositions suffisamment précises et des formules non équivoques »[141].

1.3. CADRE CONVENTIONNEL

La directive (UE) 2022/2555 (dite directive NIS 2) 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 définit en son article 6 les termes qui contribuent à déterminer son champ d'application et procède par renvoi à d'autres textes de droit dérivé de l'Union européenne, à savoir les règlements eIDAS et CSA, et ce à des fins d'harmonisation de la terminologie liée à la cybersécurité.

A titre d'exemple, la directive NIS 2 s'adresse à des prestataires de services de confiance. Aux fins d'éviter la coexistence avec une nouvelle définition propre à la directive NIS 2, celle-ci se réfère, par renvoi, à celle du règlement eIDAS.

2. NECESSITE DE LEGIFERER ET OBJECTIFS POURSUIVIS

2.1. NECESSITE DE LEGIFERER

Le présent article a pour objet de transposer les notions de la directive requises pour la mise en œuvre du dispositif normatif. Les définitions ont notamment vocation à préciser le champ d'application des obligations que porte le titre II du projet de loi et relèvent du niveau de la loi, notamment aux fins de répondre aux exigences du principe de clarté de la loi découlant de l'article 34 de la Constitution[142] d'une part et de l'objectif de valeur constitutionnelle d'accessibilité et d'intelligibilité de la loi fondé sur les articles 4, 5, 6 et 16 de la Déclaration de 1789[143].

A titre d'exemple, la notion de prestataires de services de confiance qualifiés telle que définie au présent article ne concerne que les prestataires de services de confiance qualifiés tels que définis par le règlement eIDAS. Or, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) qualifie des prestataires de services de confiance qui ne relèvent pas de du règlement eIDAS mais d'autres textes tels que l'ordonnance n° 2005-1516. Ainsi,

---

[141] Cons. const., n° 2005-514 DC, 28 avr. 2005, cons. 14.

[142] Cons. const., n° 2001-455 DC, 12 janv. 2002, cons. 9 ; n° 2001-451 DC, 27 nov. 2001, cons. 13 ; n° 98-401 DC, 10 juin 1998, cons. 10.

[143] Cons. Const., n° 2005-514 DC, 28 avr. 2005, précitée.

préciser au sein des définitions du présent article qu'au sens du titre II du projet de loi, la notion de prestataire de service de confiance est celle entendue par le règlement eIDAS permet d'éviter une surtransposition en précisant clairement le champ d'application de celle-ci.

En outre, l'adaptation de certaines notions en droit français conduisent à prévoir certaines définitions au niveau de la loi telles que celles de bureau d'enregistrement ou d'office d'enregistrement.

2.2. OBJECTIFS POURSUIVIS

S'il vise à définir les concepts et entités utiles au sens du titre II du projet de loi, ce qui limite effectivement sa portée à la mise en œuvre de la transposition de la directive NIS 2, en excluant les notions d'usage courant, l'établissement de ce bref glossaire procède également d'une démarche de simplification législative et règlementaire. Il pourrait en particulier faire office de référence pour d'autres textes, législatifs, réglementaires ou infra-réglementaires.

3. OPTIONS POSSIBLES DISPOSITIF RETENU

3.1. OPTIONS ENVISAGEES

Option 1 : Procéder par renvoi pur et simple aux définitions de la directive mais l'objectif à valeur constitutionnelle d'intelligibilité et d'accessibilité de la norme commande d'éviter, en général, la transposition par renvoi ou référence.

Option 2 : Reprendre *in extenso* l'ensemble des définitions au risque d'avoir des définitions concurrentes ou qui ne présentent pas de difficulté d'interprétation.

Option 3 : Ne reprendre que celles qui conduisent à adapter des notions existantes en droit national dès lors que le Conseil d'Etat recommande de distinguer clairement entre les termes et les notions employés par la directive qui doivent être introduits en droit interne pour les besoins de la transposition et ceux qui peuvent être transcrits par renvoi à des notions habituelles en droit français.

3.2. OPTION RETENUE

Le présent article définit huit notions courantes liées à la sécurité et à la résilience numérique, qu'il s'agisse des entités entrant dans le champ d'application du présent projet de loi ou des évènements susceptibles de les concerner :

- Bureau d'enregistrement ;
- Entité ;
- Prestataire de services de confiance ;
- Prestataire de services de confiance qualifié ;
- Office d'enregistrement ;
- Représentant ;
- Service de centre de données ;
- Système d'information.

Dans le projet de loi, il a été décidé d'inscrire les définitions qui nécessitent une éventuelle adaptation dans le droit national. C'est le cas, par exemple, des notions de bureau d'enregistrement et d'office d'enregistrement. Il a également été décidé d'inscrire celles qui permettent d'apporter une précision par rapport à cadre national. C'est le cas notamment pour les services de centre de données puisque le 11 bis de l'article L. 32 du CPCE définit le terme de « centre de données » mais la définition associée (« *On entend par centres de données les installations accueillant des équipements de stockage de données numériques.* ») est plus restrictive que celle prévue par la directive NIS 2 et reprise donc au 6° de l'article 6 du projet de loi. C'est le cas aussi de la définition de prestataires de service de confiance qualifié ou non. En France, l'ANSSI qualifie plusieurs types de service de confiance en plus de ceux prévus par le règlement n° 910/2014 dit eIDAS, comme les prestataires d'audit en sécurité des systèmes d'information (PASSI)[144]. Conformément à la directive NIS 2, qui vise uniquement les prestataires de services de confiance au sens du règlement eIDAS, seules les définitions prévues par la directive ont été reprises. Dans un souci de simplification règlementaire, une définition de système d'information a également été ajoutée au 8° du présent article parce que, comme détaillé *supra* dans le cadre général, plusieurs définitions coexistaient, notamment celle du décret n° 2019-1088 qui a été reprise dans le projet de loi.

4. ANALYSE DES IMPACTS DES DISPOSITIONS ENVISAGEES

4.1. IMPACTS JURIDIQUES

4.1.1. Impacts sur l'ordre juridique interne

Les présentes dispositions ne sont pas codifiées.

4.1.2. Articulation avec le droit international et le droit de l'Union européenne

[144] Pour consulter la liste exhaustive des services de confiance qualifiés par l'ANSSI, veuillez vous référer à cette page : Référentiels d'exigences pour la qualification | ANSSI (cyber.gouv.fr).

Au sein de ce projet de loi, il a été décidé d'inscrire les définitions de la directive NIS 2 qui nécessitent une éventuelle adaptation dans le droit national (cf. *supra*).

4.2. IMPACTS ECONOMIQUES ET FINANCIERS

4.2.1. Impacts macroéconomiques

Sans objet.

4.2.2. Impacts sur les entreprises

Sans objet.

4.2.3. Impacts budgétaires

Sans objet.

4.3. IMPACTS SUR LES COLLECTIVITES TERRITORIALES

Sans objet.

4.4. IMPACTS SUR LES SERVICES ADMINISTRATIFS

Sans objet.

4.5. IMPACTS SOCIAUX

4.5.1. Impacts sur la société

Sans objet.

4.5.2. Impacts sur les personnes en situation de handicap

Sans objet.

4.5.3. Impacts sur l'égalité entre les femmes et les hommes

Sans objet.

4.5.4. Impacts sur la jeunesse

Sans objet.

4.5.5. Impacts sur les professions réglementées

Sans objet.

4.6. IMPACTS SUR LES PARTICULIERS

Sans objet.

4.7. IMPACTS ENVIRONNEMENTAUX

Sans objet.

5. CONSULTATIONS ET MODALITES D'APPLICATION

5.1. CONSULTATIONS MENEES

Conformément aux dispositions de l'article L. 1212-2 du code général des collectivités territoriales, la présente disposition a été soumise à l'examen du Conseil national d'évaluation des normes (CNEN) qui a rendu un avis défavorable le 22 mai 2024.

Sur le fondement de l'article 8 de la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, la Commission nationale de l'informatique et des libertés (CNIL) a été consultée à titre facultatif. Elle a rendu un avis favorable le 23 mai 2024 au renforcement des mesures en matière de cybersécurité, appelant toutefois à s'assurer de la cohérence des exigences de sécurité découlant des principes relatifs à la protection des données avec celles issues de la directive NIS 2 ainsi qu'à une coordination entre la CNIL et l'ANSSI sur la mise en œuvre de NIS 2.

5.2. MODALITES D'APPLICATION

5.2.1. Application dans le temps

La disposition entrera en vigueur le lendemain de la publication du projet de loi au *Journal officiel* de la République française.

5.2.2. Application dans l'espace

Conformément à l'article 40 du présent projet de loi, le titre II est applicable dans les îles Wallis et Futuna, en Polynésie française, en Nouvelle-Calédonie et dans les Terres australes et antarctiques françaises, sous réserve des adaptations suivantes :

1° 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 applicables localement.

2° Dans les îles Wallis et Futuna, en Polynésie française et en Nouvelle-Calédonie, les sanctions pécuniaires encourues en vertu du titre II de la présente loi sont prononcées en monnaie locale, compte tenu de la contre-valeur de l'euro dans cette monnaie.

Pour l'application du titre II à Saint-Barthélemy, Saint-Pierre-et-Miquelon, dans les îles Wallis et Futuna, en Polynésie française, en Nouvelle-Calédonie et dans les Terres australes et antarctiques françaises, les références à la directive (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 et aux règlements de l'Union européenne sont remplacées par la référence aux règles en vigueur en métropole en vertu de la même directive et des mêmes règlements.

5.2.3. Textes d'application

La présente disposition ne requiert aucune mesure d'application.

Articles 7 à 16 – Périmètre de compétence de l'autorité nationale et exigences de sécurité

1. ÉTAT DES LIEUX

1.1. CADRE GENERAL

L'accroissement de la menace cybercriminelle se traduit dans les faits par un nombre croissant de victimes de cyberattaques dans tous les secteurs d'activité, publics et privés. Dans son « Panorama de la menace informatique 2023 » publié en février 2024, l'ANSSI a notamment observé une augmentation de 30 % du nombre d'attaques par rançongiciel portées à sa connaissance en 2023 par rapport à la même période en 2022.

L'Union européenne (UE) a déjà pris conscience de la nécessité de protéger les acteurs du marché unique de cette menace, afin de limiter les impacts économiques, financiers et sociétaux de la cybercriminalité, en élaborant la directive 2016/1148 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* », premier instrument du marché intérieur visant à améliorer la résilience des « *activités essentielles pour l'économie et la société de l'Union européenne* » contre les risques liés à la cybersécurité, en établissant les bases d'une cybersécurité renforcée sur un ensemble de secteurs d'activité sur le territoire de l'Union européenne.

Cette directive européenne, dite « NIS 1 » a été transposée en droit français au moyen de la loi n° 2018-133 du 26 février 2018 portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité.

Ces dispositions aujourd'hui en vigueur concernent environ 500 opérateurs, répartis dans six secteurs d'activité que l'UE avait jugés prioritaires en raison de leurs effets potentiellement systémiques (énergie, transports, banque et marchés financiers, santé, eau potable, infrastructures numériques), auxquels la France a ajouté six autres secteurs dont les enjeux ont également été jugés prioritaires (assurance, restauration, traitement des eaux, éducation, emploi et formation, organismes sociaux).

La directive est structurée autour de quatre axes principaux :

- le renforcement des capacités nationales de cybersécurité des Etats membres ;
- la coopération entre les Etats membres portant sur les aspects stratégiques et opérationnels de la cybersécurité ;

- un socle réglementaire commun pour l'identification et le renforcement, par les Etats, de la cybersécurité des opérateurs de services essentiels (OSE) dont l'interruption pourrait affecter le fonctionnement de nos économies et de nos sociétés ;
- un cadre réglementaire destiné à renforcer la cybersécurité des fournisseurs de service numérique (FSN).

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

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

Les OSE étaient désignés selon un processus, relativement lourd administrativement, impliquant la consultation des ministères sur l'identité des opérateurs à désigner, la transmission d'un courrier d'intention de désignation à chaque opérateur, une réponse officielle à la prise en compte des remarques faites par l'ANSSI puis la désignation individuelle par arrêté du Premier ministre. Le décret n° 2018-384 du 23 mai 2018 fixait notamment les règles de sécurité que les entités régulées devaient respecter, dont l'élaboration et la mise en œuvre d'une politique de sécurité des réseaux et systèmes d'information ou la détection et le traitement des incidents de sécurité affectant les réseaux et systèmes d'information.

Le texte de la première directive NIS prévoyait que la Commission réexamine périodiquement le fonctionnement global du dispositif et évalue la liste des secteurs et sous-secteurs dans lesquels sont identifiés des opérateurs de services essentiels et les types de services numériques couverts par la directive. C'est dans le respect de cet engagement que la nouvelle directive (n° 2022/2555, appelée « NIS 2 ») a été élaborée. L'évolution de son périmètre confirme au niveau européen ce que la France avait anticipé dès 2018, en intégrant des secteurs d'activité qui n'étaient pas prévus par NIS 1 et dont les entreprises désignées OSE seront automatiquement considérées comme des entités essentielles sous NIS 2.

A l'heure actuelle, certaines entités peuvent être assujetties à plusieurs régimes d'obligations en matière de cybersécurité selon qu'elles sont identifiées comme opérateur de service essentiel, OIV ou administration au sens de l'article L. 100-3 du code des relations entre le public et l'administration. Ainsi, coexistent à la fois les obligations en vertu de la loi de 2018-133, celles en vertu des articles L. 1332-6-1 du code de la défense et celles relative au respect du référentiel général de sécurité découlant de l'ordonnance n° 2005-1516.

On relève un enchevêtrement des notions et des champs d'application entre, d'une part, la directive NIS 2 et, d'autre part, les législations internes existantes, en particulier :

- Les articles L. 1332-1 et L. 1332-2 du code de la défense, qui imposent à certains opérateurs (appelés « opérateurs d'importance vitale » ou « OIV ») de mettre en œuvre des règles de sécurité nécessaires à la protection de leurs systèmes d'information pour lesquels l'atteinte à la sécurité ou au fonctionnement risquerait de diminuer d'une façon importante le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la Nation ou pourrait présenter un danger grave pour la population, obligation étendue aux systèmes d'information des opérateurs publics ou privés qui participent à ces systèmes ;
- 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 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.

Au-delà du seul champ d'application, d'autres règlementations coexistent avec la directive NIS 2. C'est le cas de l'instruction générale interministérielle 1300 (IGI 1300) relative à la protection du secret de la défense nationale. Elle a été révisée en 2021 via l'adoption d'une nouvelle version qui a fait évoluer les niveaux et modalités de classification ainsi que la procédure d'habilitation. Elle a également clarifié les modalités d'accès des acteurs privés dans un objectif général de simplification, pour répondre à la multiplication des informations et supports classifiés, et de modernisation. L'instruction interministérielle II 901 (II 901) relative à la protection des systèmes d'information sensibles implique pour les entités concernées de respecter des obligations en matière organisationnelle, d'évaluation des risques, de défense en profondeur et de respect des règles d'hygiène ainsi que de recourir à des produits de sécurité et à des prestataires de confiance qualifiés par l'ANSSI. L'instruction générale interministérielle 1337 (IGI 1337) précise le cadre de gouvernance de la sécurité numérique de l'Etat (PSSIE), aux niveaux interministériel et ministériel ainsi que pour les établissements publics sous tutelles des ministères.

1.2. CADRE CONSTITUTIONNEL

1.2.1. Principe de libre administration des collectivités territoriales

La directive NIS 2 s'applique aux administrations centrales et régionales. Par ailleurs, elle laisse la possibilité aux Etats membres d'appliquer ses dispositions aux administrations locales.

Le principe de libre administration des collectivités territoriales est consacré aux articles 34 et 72 de la Constitution de 1958 et repris dans le code général des collectivités territoriales. Il s'agit d'un principe à valeur constitutionnelle[145] qui s'impose au législateur et à toutes les autorités administratives. Le fait d'imposer des obligations aux collectivités territoriales touche au principe de leur libre administration et nécessite de légiférer[146].

1.2.2. Régime des obligations civiles et commerciales

L'article 34 de la Constitution prévoit notamment que la loi détermine les principes fondamentaux des obligations civiles et commerciales. Ainsi, une loi qui impose des obligations à des entreprises privées doit déterminer précisément le périmètre des entreprises soumises à ces obligations[147].

1.2.3. Intelligibilité de la loi

La simplification et la rationalisation du cadre législatif et règlementaire est nécessaire compte tenu de l'enchevêtrement des notions et des champs d'application entre d'une part, la directive NIS 2, et d'autre part, les législations internes existantes. En effet, l'objectif de valeur constitutionnelle d'intelligibilité de la loi assure la lisibilité des textes, prohibe la complexité « inutile »[148] et « excessive » de la loi au regard de l'aptitude de ses destinataires[149], favorise la simplification du texte législatif[150], soutient la codification, notamment à droit constant[151], combat la contradiction et l'inintelligibilité[152], et pose une exigence de précision[153].

1.2.4. Exigence de transposition des directives de l'Union européenne

Aux termes de l'article 88-1 de la Constitution : « La République participe aux Communautés européennes et à l'Union européenne, constituées d'Etats qui ont choisi librement, en vertu des traités qui les ont instituées, d'exercer en commun certaines de leurs compétences ». Le Conseil constitutionnel déduit de cette disposition que « la transposition en droit interne d'une

[145] Cons. const. 23 mai 1979, n° 79-104 DC, § 9.

[146] Cons. const. 10 mars 1988, n° 88-154 L, § 4.

[147] Cons. const. 13 août 2015, n° 2015-718 DC.

[148] Cons. const., n° 2003-473 DC, 26 juin 2003, cons. 5.

[149] Cons. const., n° 2005-530 DC, 29 déc. 2005, cons. 77.

[150] Cons. const., n° 2003-473 DC, 26 juin 2003, cons. 5 ; n° 2004-506 DC, 2 déc. 2004, cons. 5.

[151] Cons. const., n° 2003-473 DC, 26 juin 2003, cons. 5 ; n° 99-421 DC, 16 déc. 1999, cons. 13 ; n° 2004-506 DC, 2 déc. 2004, cons. 5.

[152] Cons. const., n° 2001-447 DC, 18 juill. 2001, cons. 27.

[153] Cons. const., n° 2000-437 DC, 19 déc. 2000, cons. 3.

directive communautaire résulte d'une exigence constitutionnelle »[154]. Il en va de même pour une loi ayant pour objet d'adapter le droit interne à un règlement de l'Union européenne[155].

1.3. CADRE CONVENTIONNEL

La directive NIS 2 élargit considérablement le périmètre des acteurs et secteurs régulés par la directive. En France, cela se traduit par une augmentation estimée du nombre d'entités régulées de 500 à près de 15 000, et une augmentation du nombre de secteurs régulés de 6 à 18. Elle a pour objectif d'atténuer les menaces pesant sur les réseaux et les systèmes d'information supportant les activités des entités et utilisés pour fournir leurs services, et d'assurer la continuité de ces services en cas d'incident, contribuant ainsi à la sécurité de l'Union et au bon fonctionnement de son économie et de sa société.

Le périmètre retenu dans la directive NIS 2 cible précisément les secteurs et les types d'entités ayant le plus grand impact potentiel sur l'économie et la société, là où la directive NIS 1 prévoyait une procédure nationale d'identification des opérateurs de services essentiels. Par exemple, les réseaux de communication électronique ont été intégrées dans le périmètre de la directive parce qu'ils sont considérés comme des opérateurs particulièrement sensibles aux cyberattaques en raison de leur rôle central dans les communications, le partage d'information et l'usage d'internet. C'est aussi le cas des offices d'enregistrement de noms de domaine. En fonction de leur taille et leur importance, ces opérateurs seront ensuite classés comme entité essentielle ou importante. De cette classification, la directive NIS 2, base du présent article, fait découler plusieurs obligations à la centaine d'opérateurs de réseaux de communication électronique comme la mise en place d'un cadre de gestion des risques ou l'harmonisation des modalités de remontée des incidents. Si la transposition de NIS 2 implique majoritairement des modifications du code de la défense, elle a également un impact non négligeable sur le code des postes et des communications électroniques du fait de l'intégration des réseaux télécoms.

La directive NIS 2 élargit également le périmètre des systèmes d'information à sécuriser. La focalisation du dispositif NIS 1 sur des systèmes d'information dits « essentiels » a conduit à minimiser les risques présentés par des systèmes d'information annexes ou support, dont la vocation première n'est pas de porter les applications métier au titre desquelles les opérateurs sont désignés. Or, ces systèmes constituent autant de vecteurs efficaces et fréquents d'attaques, parce qu'ils permettent d'usurper une identité numérique ou d'élever les privilèges d'un utilisateur pour lui donner accès illégalement aux actifs numériques les plus critiques de

[154] Voir notamment la décision n° 2004-496 DC du 10 juin 2004, « Loi pour la confiance dans l'économie numérique ».

[155] Voir par exemple la décision n° 2018-765, « Loi relative à la protection des données personnelles », considérant 3.

l'entité. La directive NIS 2 prévoit donc une prise en compte plus pertinente des systèmes d'information à protéger. Alors que la directive NIS 1 prévoyait une identification des systèmes d'information essentiels sur lesquels les obligations de la directive porteraient, la directive NIS 2 s'applique par défaut à l'ensemble des systèmes d'information de l'entité. Des mécanismes d'exemption de certains systèmes d'information sont toutefois permis si ces derniers n'impactent pas la réalisation des activités ou la fourniture des services de l'entité.

Enfin, bien qu'elle soit prescriptive pour un certain nombre de ses dispositions, la directive NIS 2 permet aux Etats membres d'aller plus loin que ce qu'elle prévoit de deux façons :

- soit en leur laissant le choix d'opter pour l'application des dispositions dans certains cas, par exemple pour l'intégration du niveau local ou des établissements d'enseignement supérieur ou encore la possibilité d'exempter des entités spécifiques qui exercent des activités dans les domaines de la sécurité nationale, de la sécurité publique, de la défense ou de l'application de la loi, y compris la prévention et la détection des infractions pénales, ainsi que les enquêtes et les poursuites en la matière ;
- soit en vertu du principe d'harmonisation minimale prévu à l'article 5 qui permet aux Etats membres d'adopter ou de maintenir des dispositions assurant un niveau de cybersécurité plus élevé tant qu'elles s'avèrent nécessaires, justifiées et proportionnées.

1.4. ELEMENTS DE DROIT COMPARE

La hausse des menaces cyber ne touche pas que les pays de l'Union européenne ou de l'Europe. Plusieurs Etats se sont ainsi dotés de législations en matière de cybersécurité pour faire face à ces nouvelles menaces. Le Royaume-Uni a développé une stratégie nationale de cybersécurité en 2022. Cette stratégie ne concerne cependant que les organisations gouvernementales et vise à la fois à renforcer la protection face aux risques cyber mais aussi la résilience en cas d'incident[156]. De même, les Etats-Unis ont engagé une stratégie de cybersécurité en 2023 qui est similaire à la directive NIS 2. En effet, les autorités américaines ont souhaité renforcer les exigences obligatoires qui pèsent sur les infrastructures critiques notamment les opérateurs de communications électroniques[157].

2. NECESSITE DE LEGIFERER ET OBJECTIFS POURSUIVIS

[156] National cyber strategy, UK, 2022.

[157] National cybersecurity strategy, USA, Mars 2023.

2.1. NECESSITE DE LEGIFERER

Aux termes de l'article 88-1 de la Constitution : « La République participe aux Communautés européennes et à l'Union européenne, constituées d'Etats qui ont choisi librement, en vertu des traités qui les ont instituées, d'exercer en commun certaines de leurs compétences ». Le Conseil constitutionnel déduit de cette disposition que « la transposition en droit interne d'une directive communautaire résulte d'une exigence constitutionnelle »[158]. La France a ainsi l'obligation de mettre son droit interne en conformité avec la directive européenne 2022/2555, au plus tard le 17 octobre 2024.

Cette transposition en droit français nécessite l'abrogation partielle de la loi n°2018-133 du 26 février 2018 qui transposait la directive NIS 1, laquelle est abrogée par la directive NIS 2.

En outre, la transposition de cette directive impose des obligations importantes aux entreprises et aux administrations, y compris les collectivités territoriales et leurs groupements et établissements publics, ce qui relève de l'article 34 de la Constitution (libre administration des collectivités territoriales, régime des obligations civiles et commerciales).

Les présentes dispositions permettent également d'harmoniser et de simplifier le cadre juridique existant en matière de cybersécurité en appliquant les mêmes mesures de gestion des risques et les exigences de sécurité à des systèmes d'information d'autres entités (administrations de l'Etat qui ne sont pas des entités essentielles, opérateurs d'importance vitale), aujourd'hui soumises à d'autres législations internes (ordonnance n° 2005-1516, code de la défense) qu'il convient également de modifier.

2.2. OBJECTIFS POURSUIVIS

Les objectifs sont les suivants :

- Définir le champ d'application des exigences relatives à la sécurité des systèmes d'information portées par les présentes dispositions :
    - Définir en droit national le périmètre d'application des différentes obligations, pour ce qui concerne la directive NIS 2 dans les limites de la latitude donnée aux Etats membres ;
    - Permettre à toutes les entités concernées de comprendre dans quelles conditions et à quel titre elles sont concernées par la réglementation NIS 2, sur la base de critères clairement définis et de catégories auxquelles seront associés des niveaux d'exigence adaptés ;

[158] Voir notamment la décision n° 2004-496 DC du 10 juin 2004, « Loi pour la confiance dans l'économie numérique ».

- Définir l'articulation avec les dispositions nationales et sectorielles préexistantes, qui ont également des impacts sur la cybersécurité, et préciser les conditions dans lesquelles certains opérateurs seront exclus de l'application de NIS 2, notamment au titre de clauses relatives à la sécurité nationale, mais éventuellement soumis à des obligations spécifiques au titre de la loi.

– Harmoniser, simplifier et rendre lisible le cadre juridique existant en matière de protection de certains systèmes d'information, avec des exigences de sécurité uniformisées et adaptées à chaque niveau de menace ainsi qu'aux spécificités sectorielles et thématiques. Dans les faits, cela implique de :

  - Faire des exigences de sécurité définies dans le cadre NIS 2 le socle commun applicable au plus grand nombre pour protéger nos organisations contre la menace cybercriminelle ;
  - Mettre en cohérence les exigences de sécurité supplémentaires du dispositif de sécurité des activités d'importance vitale (SAIV) destinées à protéger nos organisations les plus sensibles contre la menace stratégique, avec les exigences de sécurité NIS 2 ;
  - Traiter les besoins réglementaires spécifiques, notamment sectoriels et thématiques (comme la protection du secret), en complémentarité du bloc d'exigences NIS 2/SAIV.

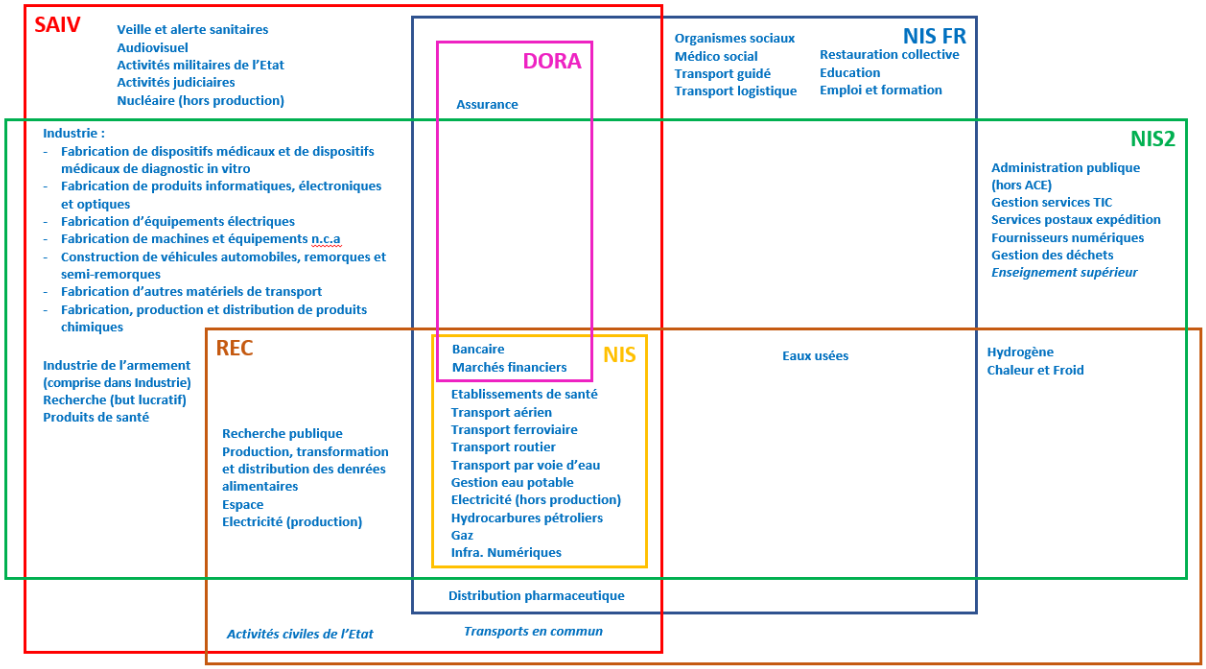


Schéma explicatif de la stratégie d'articulation du périmètre de la directive NIS 2 avec celui des autres textes existants.

3. OPTIONS ENVISAGEES ET DISPOSITIF RETENU

3.1. OPTIONS ENVISAGEES

Si les dispositions de la directive NIS 2 doivent être transposées, plusieurs options ont été envisagées s'agissant du maintien dans des textes spécifiques de dispositions relatives à la protection des systèmes d'information.

La première option consistait à ne pas intégrer dans le projet de loi les dispositions existantes dans les autres législations internes, ce qui conduisait à conserver dans la législation interne :

- Des règles de sécurité pour les systèmes d'information des entités soumises à la directive NIS 2 ;
- Des règles de sécurité spécifiques dans l'ordonnance n° 2005-1516 sur les systèmes d'information des autorités publiques, telles que définies dans cette ordonnance, lorsque ces systèmes échangent des informations avec des administrations ou des usagers ;
- Des règles de sécurité spécifiques dans le code de la défense sur les systèmes d'information d'importance vitale des opérateurs d'importance vitale (OIV) ou des systèmes d'information d'opérateurs publics ou privés qui participent à ces systèmes.

La seconde option consistait à intégrer une partie des législations existantes dans le projet de loi par l'obligation de mettre en œuvre des règles de sécurité tout en renvoyant à des textes distincts lesdites spécificités (maintien de l'ordonnance n° 2005-1516 ou des articles L. 1332-6-1 et suivants du code de la défense).

Ces options ont été écartées au profit d'une plus grande harmonisation de ces différents cadres, plus conforme à l'objectif d'intelligibilité de la loi, en intégrant l'ensemble du socle d'obligations de sécurisation ainsi que l'obligation de prévoir des règles de sécurité spécifiques pour des systèmes d'information présentant une sensibilité particulière dans un seul et même texte.

3.2. DISPOSITIF RETENU

Le dispositif retenu comprend :

- des dispositions qui explicitent les notions d'entités essentielles et d'entités importantes pour l'application des mesures de gestion des risques en matière de cybersécurité sur la base de critères objectifs (catégories d'entités, seuils/secteurs, rattachement territorial) ;
- des dispositions qui visent à fournir à l'autorité nationale de sécurité des systèmes d'information les informations nécessaires à l'établissement et à la mise à jour de la liste des entités essentielles, des entités importantes et des bureaux d'enregistrement ;

- des dispositions permettant d'assurer l'articulation avec d'autres actes juridiques sectoriels de l'Union européenne imposant eux aussi des mesures de gestion des risques en matière de cybersécurité ou de notification des incidents importants ;
- des dispositions, applicables tant aux entités essentielles et importantes qu'aux administrations de l'État et à leurs établissements publics administratifs qui ne sont pas entités essentielles, qui prévoient les objectifs des mesures de gestion des risques que ces personnes doivent mettre en œuvre en fonction des risques identifiés. Ces dispositions prévoient qu'un décret en Conseil d'État fixera les mesures de gestion des risques de cybersécurité sur leurs systèmes d'information et réseaux auxquelles doivent se conformer ces personnes et prévoira les conditions d'élaboration, de modification et de publication d'un référentiel d'exigences techniques et organisationnelles adaptées à ces différentes personnes, leur permettant, si ces dernières mettent en œuvre les exigences du référentiel, de s'en prévaloir auprès de l'autorité de contrôle pour démontrer le respect de leurs obligations ;
- des dispositions spécifiques imposant la mise en œuvre des exigences du référentiel ou de certaines exigences spécifiques sur :
    - les systèmes d'information d'importance vitale identifiés et déclarés par les OIV à l'autorité nationale de sécurité des systèmes d'information ;
    - les systèmes d'information des administrations qui sont des entités essentielles ou des entités importantes ou des administrations d'Etat et de leurs établissements publics administratifs, permettant des échanges d'informations par voie électronique entre administrations ou entre l'administration et le public.

Pour chaque objectif poursuivi, les dispositifs retenus sont les suivants :

a) <u>Périmètre d'application</u>

Les présentes dispositions prévoient une application sans restriction des éléments prescriptifs de la directive NIS 2 relatifs à la définition des entités concernées, aux critères et seuils, aux secteurs, sous-secteurs et types d'entités.

Aux termes de la directive elle-même, les entités visées par NIS 2 devraient être classées en deux catégories, entités essentielles et entités importantes, en fonction de la mesure dans laquelle elles sont critiques au regard du secteur ou du type de service qu'elles fournissent, ainsi que de leur taille.

Les articles 8 et 9 énumèrent limitativement les catégories d'opérateurs inclus dans le périmètre d'application de NIS 2, respectivement au titre des entités essentielles et des entités importantes. Ces catégories reposent en particulier sur des critères :

- de taille : les entreprises appartenant à un des secteurs d'activité hautement critiques qui emploient au moins 250 personnes ou dont le chiffre d'affaires annuel excède 50 millions d'euros ou le total du bilan annuel excède 43 millions d'euros sont des entités essentielles, alors que celles qui emploient au moins 50 personnes ou dont le total du bilan annuel excède 10 millions d'euros (et qui ne sont pas des entités essentielles) sont des entités importantes ;
- de secteur d'activité (ex. : prestataires de service de confiance qualifiés, offices d'enregistrement ou fournisseurs de services de système de noms de domaine) ;
- d'appartenance aux administrations de l'Etat, sous certaines conditions (cf. *infra*.) ;
- d'inclusion parmi les acteurs régulés au titre d'autres dispositifs : opérateurs d'importance vitale (OIV) et opérateurs de services essentiels (OSE), notamment.

La directive NIS 2 prévoit en effet à son article 3 la possibilité pour les États membres de désigner en tant qu'entités essentielles les entreprises ayant reçu le statut d'opérateur de service essentiel au titre de NIS 1. La France a en effet considéré que la mise en œuvre des mesures de cybersécurité NIS 1 a accéléré leur montée en maturité cyber ce qui, *in fine*, permettra de faciliter leur mise en conformité avec les mesures de sécurité NIS 2.

Les dispositions retiennent une déclinaison au niveau territorial du secteur des administrations publiques prenant en compte, au titre des entités essentielles, les régions, conformément à la directive qui vise expressément les administrations au niveau régional comme relevant d'un secteur hautement critique. En revanche, elle laisse le choix d'une application des dispositions de la directive au niveau local (cf. article 2 § 5 a). Dans une même approche de proportionnalité qui irrigue la directive, les dispositions du projet de loi s'attachent à intégrer le niveau local, lorsqu'il présente une sensibilité particulière le justifiant. Cela concerne notamment les départements, métropoles, communautés urbaines, communautés d'agglomérations, et communes de plus de 30 000 habitants, ainsi que leurs établissements publics administratifs dont les activités s'inscrivent dans un des secteurs d'activité hautement critiques ou critiques. Sont également compris dans ce périmètre les centres de gestion, services départementaux d'incendie et de secours, les syndicats dont les activités s'inscrivent dans un des secteurs d'activité hautement critiques ou critiques et dont la population bénéficiaire est supérieure à 30 000 habitants ou encore les institutions et organismes interdépartementaux dont les activités s'inscrivent dans un des secteurs d'activité hautement critiques ou critiques. Les communautés de communes et leurs établissements publics administratifs dont les activités s'inscrivent dans un des secteurs d'activité hautement critiques ou critiques, sont quant à elles incluses au titre des entités importantes.

La directive, à son article 2 §5 b), prévoit que les établissements d'enseignement peuvent être inclus sur décision des Etats membres. Les articles 8 et 9 ne retiennent dans leur champ d'application, au titre des entités essentielles ou importantes, selon les cas, que les seuls établissements d'enseignement supérieur menant des activités de recherche.

Le texte prévoit par ailleurs l'intégration dans le périmètre, comme entités essentielles, des opérateurs déjà désignés opérateurs de service essentiel (OSE) au titre de NIS 1.

Il maintient également le pouvoir de désignation unitaire, par arrêté du Premier ministre, d'entités dont le niveau de criticité, estimé en concertation avec les ministères coordonnateurs, le justifie, sans considération des seuils de chiffre d'affaires ou de nombre d'employés applicables dans le cadre général.

L'article 10 prévoit enfin de mettre en œuvre le « sur-classement » laissé à l'appréciation des Etats membres sur la base des critères définis par la directive NIS 2 (à son article 3 1° e). Ce mécanisme permet de désigner comme entité essentielle une entité dont l'évaluation de criticité le justifie sur le plan national, alors que les conditions relatives à son secteur d'activité ou à sa taille la destinaient à être considérée en tant qu'entité importante par le texte de la directive.

La transposition française exclut du périmètre d'application, conformément au 7° de l'article 2 relatif au champ d'application de la directive NIS 2, les entités de l'administration publique qui exercent leurs activités dans les domaines de la sécurité nationale, de la sécurité publique, de la défense ou de l'application de la loi, en particulier celles de l'administration régalienne.

A son article 14, le projet de loi prévoit cependant de leur appliquer des mesures de droit national équivalentes aux obligations découlant de NIS 2, à l'exception du principe de remontée d'information au niveau européen prévu par la directive. Cela implique de mettre en place un pilotage de la sécurité des réseaux et systèmes d'information adaptée, comprenant notamment la formation à la cybersécurité des membres des organes de direction et des personnes exposées aux risques, d'assurer la protection des réseaux et systèmes d'information, y compris en cas de recours à la sous-traitance, de mettre en place des outils et des procédures pour assurer la défense des réseaux et systèmes d'information et gérer les incidents et de garantir la résilience des activités.

b) Articulation avec les autres réglementations

La transposition française prévoit, à son article 13, l'application des clauses incluses dans la directive NIS 2, relatives à la notion d'acte juridique sectoriel de l'Union.

Elle prend en compte l'évolution nécessaire du dispositif SAIV, pour que toute entité désignée OIV soit soumise aux obligations afférentes au statut d'entité essentielle, ainsi qu'à des obligations spécifiques visant à les protéger de la menace stratégique/étatique ciblée (la directive NIS 2 visant une protection contre la menace cybercriminelle de masse). Le projet de loi prévoit de conserver et de faire évoluer des obligations complémentaires spécifiques au statut d'OIV.

c) Conditions de mise en œuvre

Les entités concernées par la directive NIS 2 ne seront pas désignées par l'administration, contrairement à ce qui était prévu par la directive NIS 1. Elles devront analyser les critères et seuils qui permettent de définir si elles sont ou non assujetties à cette nouvelle réglementation, et le cas échéant devront prendre l'initiative de s'enregistrer auprès de l'autorité nationale de cybersécurité compétente. Cet enregistrement consistera à identifier l'entité et les critères au titre desquels elle est concernée, et de porter à la connaissance de l'autorité nationale de sécurité des systèmes d'information toutes les informations qui permettront l'échange entre autorité et assujetti, l'accompagnement à la mise en œuvre, le contrôle, les injonctions et les sanctions.

4. ANALYSE DES IMPACTS DES DISPOSITIONS ENVISAGEES

4.1. IMPACTS JURIDIQUES

4.1.1. Impacts sur l'ordre juridique interne

Les présentes dispositions de transposition prévoient, en application de cette possibilité, des obligations pour les régions, les départements, les grandes communes et certains groupements mais également pour certains établissements publics locaux.

Les présentes mesures créent de nouvelles dispositions qui ne seront pas codifiées.

Ces dispositions impliquent des modifications de législations existantes :

- pour intégrer les obligations de la directive NIS 2 qui abroge la directive NIS 1. Cela implique l'abrogation des articles 1 à 15 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 systèmes d'information d'importance vitale qui transposaient la directive NIS 1 ;
- pour harmoniser et simplifier le cadre juridique national existant :
    - ainsi, dans le cadre du remplacement du chapitre II du titre III du Livre III de la partie 1 du code de la défense, les dispositions applicables aux systèmes d'information (nouvel article L. 1332-13) renvoient aux dispositions de la loi sur les exigences spécifiques applicables aux systèmes d'information d'importance vitale ;
    - les obligations relatives à la mise en œuvre de fonctions de sécurité sur les systèmes d'information des autorités administratives 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 sont

supprimées (suppression des quatrième et cinquième alinéas de l'article premier, abrogation des articles 9 et 12, suppression du premier alinéa de l'article 14).

4.2. IMPACTS ECONOMIQUES ET FINANCIERS

4.2.1. Impacts macroéconomiques

Pour l'économie et la société françaises, la mise en conformité des entités régulées permettra d'atteindre un niveau de sécurité renforcé pour adresser la cybercriminalité de masse, qui aura nécessairement pour effets de complexifier la tâche des attaquants et de diminuer, à leurs yeux, l'attrait des entités régulées.

Le périmètre d'application retenu dans la transposition française tient compte des effets systémiques d'une attaque, c'est-à-dire généralisés et étendus à l'ensemble d'un secteur et aux autres secteurs qui peuvent en dépendre.

Par conséquent, le périmètre retenu dans le projet de loi cible précisément les secteurs et les types d'entités ayant le plus grand impact potentiel sur l'économie française. La durée d'indisponibilité des services d'une entité, constatée sur de nombreux exemples d'attaques qui ont donné lieu à des opérations de cyberdéfense conduites par l'ANSSI, varie de quelques semaines à plusieurs mois, selon le niveau de préparation de l'entité victime. L'application de la réglementation NIS 2 au périmètre retenu permettra de limiter la probabilité et la durée des interruptions de service, et donc la perte de chiffre d'affaires, voire le risque de faillite pour les entités à but lucratif, sur les secteurs essentiels au bon fonctionnement de notre économie : électricité, transports, banque et infrastructures de marchés financiers, infrastructures numériques, espace, services postaux et d'expédition, industrie manufacturière, transformation et distribution des denrées alimentaires, etc.

L'augmentation du niveau de sécurisation des acteurs économiques constitue également un facteur de compétitivité, dans la mesure où les donneurs d'ordres s'orientent plus volontiers vers des producteurs ou des prestataires dont la maitrise des moyens de production inspire confiance. Cela procure en effet des garanties en termes de disponibilité et donc de respect des délais contractuels, de protection des données, potentiellement stratégiques, confiées dans le cadre d'une prestation, et de fiabilité dans le résultat produit, la vulnérabilité des moyens de production à une attaque cyber pouvant aboutir à la corruption des produits livrés.

4.2.2. Impacts sur les entreprises

Pour les entités régulées, dont le nombre est estimé à environ 15 000, la mise en conformité au regard de la réglementation NIS 2 nécessitera un investissement initial, qui se traduira notamment par une mobilisation de compétences. Le maintien global en conditions de sécurité

des systèmes d'information critiques devra aussi faire l'objet d'un flux financier annuel, pour adapter en continu le dispositif aux évolutions du système d'information et à la menace, sans que l'impact de la nouvelle réglementation sur des dépenses *a priori* déjà prévues puisse être spécifiquement identifié.

Il convient en effet de relativiser cet effort nécessaire pour la mise en conformité, pour deux raisons notamment :

- les entités essentielles sont des structures déjà sensibilisées ou confrontées à la menace cyber. Elles seront pour partie des opérateurs de services essentiels (OSE), et donc déjà soumises depuis plusieurs années à la réglementation NIS 1. A ce titre, l'effort pour se conformer à NIS 2 devrait être limité. Celles qui ne sont pas déjà OSE sont pour la plupart des entités dont les critères de taille et de chiffre d'affaires les situent dans une catégorie pour laquelle la dépendance aux infrastructures numériques ne fait pas de doute et qui ont déjà, à ce titre, développé une certaine maîtrise de leur sécurité numérique.
- le niveau d'exigence requis vis-à-vis des entités importantes a été conçu pour diminuer leur probabilité d'être atteintes par un rançongiciel courant vis-à-vis duquel elles seraient désemparées, sans nécessiter des investissements disproportionnés. Une certaine latitude leur sera par ailleurs laissée pour adopter des modalités de mise en œuvre des recommandations de sécurité les plus adaptées à leur connaissance des impacts potentiels d'une attaque, à leur environnement éventuellement spécifique, ainsi qu'à leurs moyens. Le niveau d'ambition pour les entités importantes n'excèdera donc pas celui des règles d'hygiène informatique largement préconisées par l'ANSSI relatives notamment à la sensibilisation et formation des utilisateurs, à la connaissance du systèmes d'information, au contrôle des accès ou à la sécurité des postes, du réseau et de l'administration[159]. En outre, le « Règlement général sur la protection des données » (RGPD) en vigueur depuis mai 2018, invite les entités à mettre en œuvre des mesures de sécurité sur lesquelles elles peuvent capitaliser pour atteindre les objectifs posés par NIS 2. Enfin, des économies d'échelle sont possibles, notamment pour les mesures organisationnelles, par exemple par la mutualisation ou l'externalisation de la fonction de RSSI (« *RSSI as a Service* »).

Il convient par ailleurs de mettre en perspective les investissements nécessaires pour se mettre en conformité avec les dispositions de NIS 2, au regard du coût constaté d'une cyberattaque par rançongiciel. Dans la sphère publique, les établissements hospitaliers ont supporté les dégâts les plus élevés : les coûts directs ont ainsi été estimés à 2,36 millions d'euros pour le Centre hospitalier Dax-Côte d'Argent (février 2021) et à plus de 5,5 millions pour le Centre

[159] ANSSI, Guide d'hygiène informatique « Renforcer la sécurité de son système d'information en 42 mesures » dont la deuxième version a été publiée en septembre 2017.

hospitalier Sud-Francilien de Corbeil-Essonnes (août 2022). Les collectivités territoriales et les intercommunalités ont également été lourdement affectées, avec des coûts directs estimés à 960 000 euros pour la Métropole Aix-Marseille-Provence (mars 2020) et à plus de 1,5 millions d'euros pour la ville de Bondy (novembre 2020).

4.2.3. Impacts budgétaires

Au niveau des administrations publiques nationales, les dernières évaluations du niveau de cybersécurité montrent un certain retard de ce secteur par rapport au secteur privé. Une hausse limitée de leur plafond d'appui, susceptible de s'appuyer sur la réinternalisation en cours de certaines compétences numériques, pourrait permettre d'adresser cet écart, dont la gestion s'inscrit notamment dans la logique de la feuille de route de cybersécurité et du cadre de gouvernance de la sécurité numérique de l'état mise en place par le décret n° 2022-513 du 8 avril 2022 relatif à la sécurité numérique du système d'information et de communication de l'Etat et de ses établissements publics.

4.3. IMPACTS SUR LES COLLECTIVITES TERRITORIALES

1489 entités, collectivités territoriales et groupements de collectivités territoriales (661), ainsi que certains organismes sous leur tutelle devraient être concernés au titre des entités essentielles :

- les régions métropolitaines ainsi que les régions et les « pays et territoires d'outre-mer » (22 entités) ;
- les départements métropolitains et d'outre-mer (97 entités) ;
- les métropoles, communautés urbaines et communautés d'agglomérations métropolitaines et d'outre-mer (263 entités) ;
- les communes de plus de 30 000 habitants métropolitaines et d'outre-mer (279 entités) ;
- les centres de gestion (104 entités) ;
- les services départementaux d'incendie et de secours ;
- les syndicats dont les activités s'inscrivent dans un des secteurs d'activité hautement critiques ou critiques et dont la population bénéficiaire est supérieure à 30 000 habitants.

Les 992 communautés de communes métropolitaines et d'outre-mer seront quant à elles concernées au titre des entités importantes.

La très grande majorité des communes (99% ont moins de 30 000 habitants) ne sont donc concernées que par leur intercommunalité de rattachement.

Les collectivités concernées devront donc monter en compétences sur le sujet de la cybersécurité.

4.4. IMPACTS SUR LES SERVICES ADMINISTRATIFS / L'AUTORITE NATIONALE

La mise en œuvre de la nouvelle réglementation NIS 2 aura plusieurs effets sur les services concernés par la cybersécurité au niveau national.

L'articulation de la réglementation NIS 2 avec les autres réglementations sectorielles ou nationales vise à simplifier globalement la mise en œuvre de la cybersécurité en France, notamment en limitant l'effet d'empilement d'exigences réglementaires. En ce sens, les présentes dispositions auront des impacts limités à l'égard des services administratifs. Les activités de sensibilisation, formation, accompagnement et régulation pourront en partie être mutualisées dans la mesure où les exigences relevant de différents statuts procèderont de référentiels communs et cohérents. Ce sera notamment le cas concernant les entités essentielles, les administrations publiques nationales et les opérateurs d'importance vitale, actuellement soumis à trois corpus réglementaires distincts, qui évolueront pour converger vers un ensemble partagé de règles construites en réponse à des objectifs communs. Ainsi les ministères ne seront plus sollicités par le processus de désignation d'OSE qui disparaîtra et avec lequel disparaitront des charges administratives lourdes de formalisme : consultation des ministères sur l'identité des opérateurs à désigner, transmission d'un courrier d'intention de désignation à chaque opérateur, réponse officielle à la prise en compte de ses remarques, désignation individuelle par arrêté du Premier ministre.

Pour l'autorité nationale de sécurité des systèmes d'information, l'extension massive du périmètre se traduira automatiquement par une multiplication d'un facteur d'environ 20 à 30 du nombre total d'entités régulées. Les réglementations de cybersécurité de cette nature s'appliquent actuellement à environ 600 opérateurs (OIV et OSE), l'organisation actuelle de l'autorité nationale étant dimensionnée pour entretenir une relation de relative proximité avec eux, justifiée par la mise en œuvre de cadres de régulation relativement récents. Le changement d'échelle induit par les critères retenus dans la directive NIS 2 ne sera cependant pas répercuté dans les mêmes proportions au sein de l'autorité nationale. Les mécanismes de régulation retenus, et notamment celui prévu à l'article 12 consistant à demander aux entités assujetties de se déclarer elles-mêmes auprès de l'autorité nationale, permettront d'alléger la charge de travail administratif de l'autorité. Par ailleurs, l'expérience de plusieurs années d'accompagnement et d'évaluation permet à l'autorité nationale de développer des outils numériques afin d'automatiser une importante partie de la relation avec les assujettis, ce qui limitera également le besoin de renfort en effectif. L'autorité nationale envisage de surcroît

d'utiliser des relais, notamment sectoriels, qui faciliteront les échanges d'information avec les entités régulées et allégeront par conséquent la charge de sensibilisation actuelle.

Le renforcement d'effectif nécessaire pour que l'autorité nationale assume ses missions au regard de l'évolution du périmètre restera raisonnable, de l'ordre de 60 ETP.

Les objectifs de sécurité envisagés pour les entités essentielles sont une évolution des règles proposées pour NIS 1 pour lesquelles il existe majoritairement des guides pour aider les organisations à leur mise en œuvre. L'effort de sensibilisation réalisé par l'ANSSI dans la mise en œuvre de la loi de programmation militaire de 2014 et de NIS 1 a permis d'accompagner de nombreuses entités à leur mise en conformité. Ces entités pourront servir de relais pour accompagner leur chaîne de sous-traitants.

L'ANSSI renforce également, dans la perspective de la mise en œuvre de NIS 2, son action vis-à-vis des fédérations professionnelles, des associations professionnelles des acteurs de la cybersécurité, et anime des communautés de prestataires de services qualifiés dans un objectif d'accompagnement à la fois des futures entités régulées à leur mise en conformité, mais également des offreurs de produits et services pour qu'ils proposent des parcours d'accompagnement adaptés.

4.5. IMPACTS SOCIAUX

4.5.1. Impacts sur la société

La réglementation NIS 2 engendre des obligations sur un grand nombre d'activités au sein de l'UE, ce qui nécessite de mobiliser de nombreuses compétences en cybersécurité, allant des plus techniques, comme les tests de pénétration de réseaux ou les investigations suite à incident, à celles relatives à la gouvernance, comme la gestion de crise, ou à des connaissances méthodologiques, comme les analyses de risque. Elle constitue par conséquent une opportunité de création d'emplois, dont on sait qu'ils seront pérennes à la fois chez les entités régulées privées, au sein des administrations et dans les équipes des prestataires de services en cybersécurité, de plus en plus sollicités.

4.5.2. Impacts sur les personnes en situation de handicap

Sans objet.

4.5.3. Impacts sur l'égalité entre les femmes et les hommes

Ce besoin supplémentaire de compétences en cybersécurité ne fait que grossir celui déjà identifié plus largement dans les métiers du numérique. Une des façons d'accroitre le volume de la main d'œuvre qualifiée disponible consiste à encourager les femmes à s'engager dans

les métiers du numérique et de la cybersécurité, alors que leur niveau de représentation à la fois en entreprises et dans les organismes de formation est particulièrement bas. Sans être un facteur de succès suffisant, les besoins de compétences accrues portés par la nouvelle réglementation cyber auront indirectement un effet favorable à une meilleure mixité femmes-hommes.

4.5.4. Impacts sur la jeunesse

Sans objet.

4.5.5. Impacts sur les professions réglementées

Sans objet.

4.6. IMPACTS SUR LES PARTICULIERS

Sans objet.

4.7. IMPACTS ENVIRONNEMENTAUX

Le dispositif retenu permet de prendre en compte dans le périmètre réglementaire une grande partie des sites industriels présentant des risques d'accidents majeurs au sens de la directive SEVESO, bien que tous ces acteurs ne puissent être regroupés dans un seul secteur, au sens de la nomenclature NIS 2. Les mécanismes de désignation unitaire et de sur-classement permettent en effet de faire entrer dans le périmètre d'application les entités dont les activités sont en relation avec des substances dangereuses pour la santé et pour l'environnement. La sécurisation de leurs systèmes informatiques apportera une garantie supplémentaire dans la gestion de leurs risques industriels.

Le fait que les secteurs des eaux usées (« hautement critique » au sens de l'annexe I de la directive) et de la gestion des déchets (« critique ») entrent dans le périmètre NIS 2 aura pour effet de sécuriser les processus industriels de recyclage ou de traitement, et de renforcer la résilience des acteurs environnementaux correspondant.

Les présentes dispositions présentent peu d'impacts directs complémentaires sur l'environnement, même si on peut considérer que la sécurisation efficace des infrastructures et des services numériques, y compris en environnement industriel, aura pour effet de contenir la consommation de papier (bureautique) et de matières premières (processus industriels), et de limiter les déplacements des personnels (télétravail et téléconférences).

5. CONSULTATIONS ET MODALITES D'APPLICATION

5.1. CONSULTATIONS MENEES

Dans une logique de co-construction, l'ANSSI a conduit un grand nombre de consultations préalables à la transposition de la directive européenne 2022/2555.

Les prestataires qualifiés par l'ANSSI pour réaliser des accompagnements au profit des actuels opérateurs régulés (OIV et OSE) ont fait partie des premières consultations. Les échanges avec ces prestataires (PASSI : prestataires d'audit de la sécurité des systèmes d'information ; PRIS : prestataires de réponse aux incidents de sécurité ; PDIS : prestataires de détection d'incidents de sécurité) ont permis de bénéficier d'un retour d'expérience sur les difficultés et le coût de mise en conformité de leurs clients avec les réglementations SAIV et NIS. Cette consultation a également donné lieu à l'expression d'avis pertinents étayés par la connaissance des réalités de terrain, sur les niveaux de sécurisation souhaitables et supportables qui pourraient être imposés aux entités assujetties à NIS 2, selon leur taille.

Les associations professionnelles représentatives des secteurs constituant le périmètre de NIS 2 ont été sollicitées en trois étapes pour recueillir, analyser et synthétiser les avis de leurs adhérents. Un peu plus de 70 fédérations ont ainsi participé dans le courant du second semestre 2023 à ces consultations sur les définitions de périmètre, les modalités d'échange entre autorité nationale et assujettis, et concernant les mesures de cybersécurité qui seront intégrées dans la réglementation nationale.

Les associations d'élus et des représentants des collectivités territoriales ont quant à elles été consultées pour déterminer, en ce qui les concerne, un périmètre pertinent d'application de la directive, comprendre les difficultés auxquelles elles pourraient être confrontées et identifier les accompagnements spécifiques qu'elles pourraient nécessiter pour les aider à atteindre les niveaux de conformité attendus.

En application de l'article L. 1212-2 du CGCT, les dispositions envisagées ont été soumises à titre obligatoire au Conseil national d'évaluation des normes, qui a rendu un avis défavorable le 22 mai 2024.

La Commission supérieure du numérique et des postes a été consultée sur les présentes dispositions. Elle a rendu un avis n° 2024-03 le 21 mai 2024 appelant à s'assurer de la clarté du périmètre des entités concernées et des mesures qu'elles devront appliquer ainsi qu'à mettre en œuvre une stratégie d'accompagnement à la mise en conformité et une politique de supervision progressive.

Sur le fondement de l'article 8 de la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, la Commission nationale de l'informatique et des libertés a été consultée à titre facultatif. Elle a rendu un avis favorable le 23 mai 2024 au

renforcement des règles en matière de cybersécurité, appelant toutefois à s'assurer de la cohérence des exigences de sécurité découlant des principes relatifs à la protection des données avec celles issues de la directive NIS 2 ainsi qu'à une coordination entre la CNIL et l'ANSSI sur la mise en œuvre de NIS 2.

5.2. MODALITES D'APPLICATION

5.2.1. Application dans le temps

Telle que prévue par la directive NIS 2, la transposition française entrera en application au plus tard le 17 octobre 2024, date de l'échéance de transposition.

La disposition entrera en vigueur le lendemain de la publication de la loi au *Journal officiel* de la République française.

Dès l'entrée en vigueur de la loi, les entités concernées auront l'obligation de s'enregistrer auprès de l'autorité nationale de cybersécurité.

La réglementation NIS 2, telle que mise en œuvre en France, définira des délais de mise en conformité qui tiendront compte des efforts de compréhension, de montée en compétence et d'investissement que les exigences imposent aux assujettis. Les lignes directrices et les objectifs de haut niveau font partie des textes publiés depuis fin 2022, mais les textes précis de transposition ne seront connus du grand public qu'à la suite de la phase règlementaire. Une mise en œuvre de contrôles susceptibles de découler sur des sanctions n'est pas envisagée avant plusieurs années.

5.2.2. Application dans l'espace

Les dispositions de transposition de la directive NIS 2, applicable dans l'ensemble de l'Union européenne, s'appliquent sur l'ensemble du territoire national. Des dispositions réglementaires particulières seront prévues pour couvrir les collectivités territoriales à statut particulier (notamment Outre-mer) et selon le principe de spécialité législative.

Conformément à l'article 40 du présent projet de loi, le titre II, à l'exception de l'article 13, est applicable dans les îles Wallis et Futuna, en Polynésie française, en Nouvelle-Calédonie et dans les Terres australes et antarctiques françaises, sous réserve des adaptations suivantes :

1° 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 applicables localement.

2° Dans les îles Wallis et Futuna, en Polynésie française et en Nouvelle-Calédonie, les sanctions pécuniaires encourues en vertu du titre II de la présente loi sont prononcées en monnaie locale, compte tenu de la contre-valeur de l'euro dans cette monnaie.

L'article 13 du titre II n'est pas applicable à Saint-Barthélemy et à Saint-Pierre-et-Miquelon.

Pour l'application du titre II à Saint-Barthélemy, Saint-Pierre-et-Miquelon, dans les îles Wallis et Futuna, en Polynésie française, en Nouvelle-Calédonie et dans les Terres australes et antarctiques françaises, les références à la directive (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 et aux règlements de l'Union européenne sont remplacées par la référence aux règles en vigueur en métropole en vertu de la même directive et des mêmes règlements.

5.2.3. Textes d'application

Un décret en Conseil d'Etat précise :

- la liste des secteurs d'activité hautement critiques et critiques ;
- certains critères d'identification des entités essentielles et importantes ;
- les modalités de désignation unitaire de certaines entités par le Premier ministre ;
- les modalités de communication des informations nécessaires à l'établissement de la liste des entités ;
- l'application des mesures de sécurité.

Par arrêté du Premier ministre, certaines entités seront désignées comme entités essentielles ou importantes ou exclues du champ du texte.

Articles 18 à 22 – Enregistrement des noms de domaine

1. ETAT DES LIEUX

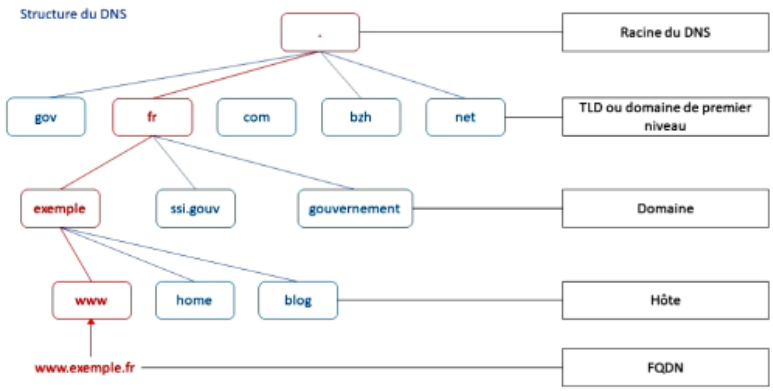
1.1. CADRE GENERAL

Le « *Domain Name System* » (système de nom de domaine) ou DNS est un service permettant de faire correspondre un nom de domaine à une adresse IP (Internet Protocol) – le numéro attribué à titre permanent ou provisoire à chaque périphérique relié à Internet, adresse qui prend la forme d'une suite de numéros (par exemple, « 45.60.12.53 ») et est compréhensible par une machine.

Le nom de domaine (URL ou *Uniform Resource Locator*s, « localisateur uniforme de ressource », sous la forme « exemple.fr »), plus facile à retenir et à retranscrire pour l'internaute, constitue l'alias alphanumérique de l'adresse IP. Les machines appelées serveurs de nom de domaine (ou serveurs DNS) permettent d'établir la correspondance entre le nom de domaine et l'adresse IP des machines d'un réseau.

Le système DNS s'appuie sur une structure arborescente. L'ensemble des noms de domaine constituent ainsi un arbre inversé où chaque nœud est séparé du suivant par un point. On appelle « nom de domaine » chaque nœud de l'arbre. Le nom absolu, correspondant à l'ensemble des étiquettes des nœuds d'une arborescence, séparées par des points, et terminé par un point final, est appelé adresse FQDN (Fully Qualified Domain Name). A titre d'exemple, « legifrance.gouv.fr. » constitue une adresse FQDN.

Lorsqu'une requête relative à un nom de domaine est effectuée, des serveurs sont successivement interrogés pour retrouver l'adresse IP correspondante. Si l'on cherche par exemple le nom de domaine « exemple.fr », dans un premier temps, un serveur racine est interrogé, qui renvoie vers le serveur faisant autorité pour le domaine de premier niveau, appelé le *Top Level Domain* ou extension (« .fr » dans l'exemple). Dans un second temps, le serveur autorité de premier niveau renvoie l'adresse du serveur faisant autorité sur le second niveau (ici, « exemple.fr »), et cela jusqu'à ce que la requête soit résolue.



Le domaine de premier niveau est, dans le système de noms de domaine internet, un sous domaine de la racine. Il est possible de les distinguer en trois principales catégories :

- domaine de premier niveau spécial (à des fins techniques, tel le « .arpa » relatif aux paramètres d'adressage et de routage) ;
- domaines de premier niveau nationaux (correspond à un pays ou un territoire de celui-ci. Ex : « .fr », « .nc ») ;
- domaines de premier niveau génériques (correspond en général à un secteur d'activité). Ces domaines se divisent en domaines génériques non parrainés (« .net », « .org » pour les organisations à but non lucratif, « .com » pour les organisations à but lucratif, « .pro » etc…) et en domaines génériques parrainés (« .gov » pour les organismes gouvernementaux américains).

Chaque domaine de premier niveau est géré par une organisation qui est chargée d'allouer (éventuellement de manière commerciale) ses sous-domaines, aussi appelée office d'enregistrement.

Cet office d'enregistrement est une entité à laquelle un domaine de premier niveau spécifique a été délégué et qui est responsable de l'administration du domaine de premier niveau, y compris de l'enregistrement des noms de domaine relevant du domaine de premier niveau et du fonctionnement technique du domaine de premier niveau, notamment l'exploitation de ses serveurs de noms, la maintenance de ses bases de données et la distribution des fichiers de zone du domaine de premier niveau sur les serveurs de noms, que ces opérations soient effectuées par l'entité elle-même ou qu'elles soient sous-traitées, mais à l'exclusion des situations où les noms de domaine de premier niveau sont utilisés par un registre uniquement pour son propre usage. A titre d'exemple, en application de l'article L. 45 du code des postes et des communications électronique, l'office d'enregistrement en charge du domaine de premier niveau du « .fr » est l'Association française pour le nommage Internet en coopération

(AFNIC)[160], qui agit sur délégation du ministre chargé des communications électroniques. Dans cet environnement, les bureaux d'enregistrement, qui sont des entités fournissant des services d'enregistrement de noms de domaine, exercent leur activité d'intermédiaire auprès de l'office d'enregistrement d'une part et des professionnels et particuliers d'autre part. Ils sont accrédités par les offices d'enregistrement à cette fin. A titre d'illustration, l'AFNIC répertorie comme bureaux d'enregistrement Orange, SFR (pour les fournisseurs d'accès à internet), Gandi, OVH ou bien encore Nameshield.

Cadre réglementaire actuel pour les noms de domaines de premier niveau :

Au niveau national :

Aujourd'hui, le seul cadre juridique existant relatif aux noms de domaine est celui prévu par le CPCE aux articles L. 45 à L. 45-8. Il est relatif à l'enregistrement et à l'attribution des seuls noms de domaine de premier niveau (« .fr »).

Au niveau européen :

La directive NIS 1 ne prévoyait pas, dans son champ d'application, d'obligations pour les bureaux d'enregistrement, ni de dispositions relatives à la sécurisation des noms de domaines génériques.

La directive NIS 2, en ce sens, opère un changement en intégrant 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.

Afin d'harmoniser les règles à l'échelle européenne et de pouvoir accéder aux données permettant d'identifier le propriétaire d'un nom de domaine en cas d'incident, l'article 28 de la directive NIS 2 prévoit de nouvelles règles en matière d'enregistrement des noms de domaine. Les Etats membres doivent imposer aux offices d'enregistrement de collecter et de conserver certaines données d'enregistrement des noms de domaine (nom du titulaire, point de contact, nom du domaine…) et organise l'accès et la publicité de ces données. La directive prévoit également que les Etats membres doivent prendre des mesures pour s'assurer de la fiabilité des serveurs et des bases de données des offices d'enregistrement des noms de domaine.

1.2. CADRE CONSTITUTIONNEL

[160] Arrêté du 20 septembre 2021 désignant l'office d'enregistrement chargé d'attribuer et de gérer les noms de domaine au sein des domaines de premier niveau du système d'adressage par domaines de l'internet correspondant au « .fr ».

Aux termes de l'article 88-1 de la Constitution : « La République participe à l'Union européenne constituée d'Etats qui ont choisi librement d'exercer en commun certaines de leurs compétences en vertu du traité sur l'Union européenne et du traité sur le fonctionnement de l'Union européenne, tels qu'ils résultent du traité signé à Lisbonne le 13 décembre 2007 ». Le Conseil constitutionnel déduit de cette disposition que : « la transposition en droit interne d'une directive communautaire résulte d'une exigence constitutionnelle »[161].

L'article 74 de la Constitution prévoit que les modalités d'application des lois dans les collectivités d'outre-mer reposent sur une loi organique. En modifiant l'applicabilité des mesures dans les collectivités d'outre-mer, le législateur s'inscrit dans ce cadre constitutionnel et devra, à ce titre, veiller à sa compatibilité avec le statut qui régit chaque collectivité sous peine de censure[162].

En ce qui concerne particulièrement les noms de domaine, le Conseil constitutionnel dans sa décision n° 2010-45 QPC[163] a estimé que l'encadrement, tant pour les particuliers que pour les entreprises, du choix et de l'usage des noms de domaine sur internet affecte les droits de la propriété intellectuelle, la liberté de communication et la liberté d'entreprendre.

- S'agissant des droits de la propriété intellectuelle, leur rattachement à la protection constitutionnelle des articles 2 et 17 de la Déclaration de 1789 s'est fait en deux temps. Le Conseil a d'abord reconnu la protection la propriété industrielle et commerciale, en 1991[164]. Dans un second temps, le Conseil a consacré l'extension de cette protection constitutionnelle aux droits de la propriété culturelle[165]. Enfin, le Conseil a précisé la portée de la protection constitutionnelle des droits d'auteur, compris comme « le droit, pour les titulaires du droit d'auteur et de droits voisins, de jouir de leurs droits de propriété intellectuelle et de les protéger dans le cadre défini par la loi et les engagements internationaux de la France »[166]. Dans la motivation de sa décision du 6 octobre 2010 précitée, le Conseil constitutionnel relève que l'encadrement du choix et de l'usage des noms de domaine affecte les droits de la propriété intellectuelle ;

- Dans sa décision 2009-580 DC précitée, le Conseil a conféré une valeur forte au droit d'accéder à l'internet comme un droit attaché à l'article 11 de la Déclaration des droits de l'homme et du citoyen de 1789 en jugeant « qu'en l'état actuel des moyens de communication et eu égard au développement généralisé des services de

[161] CC, décision n° 2004-496 DC du 10 juin 2004, Loi pour la confiance dans l'économie numérique.

[162] CC, décision n° 80-122 DC, 22 juillet 1980, Loi rendant applicable le Code de procédure pénale et certaines dispositions législatives dans les territoires d'outre-mer.

[163] CC, décision n° 2010-45 QPC, 6 octobre 2010, *M. Mathieu P. [Noms de domaine Internet]*.

[164] CC, décision n° 90-283 DC du 8 janvier 1991.

[165] CC, décision n° 2006-240 DC du 27 juillet 2006.

[166] CC, décision n° 2009-580 DC du 10 juin 2009.

communication au public en ligne ainsi qu'à l'importance prise par ces services pour la participation à la vie démocratique et l'expression des idées et des opinions, ce droit implique la liberté d'accéder à ces services ». Il reprend ce raisonnement dans sa décision n° 2010-45 QPC précitée et juge ainsi « qu'en l'état actuel des moyens de communication et eu égard au développement généralisé des services de communication au public en ligne ainsi qu'à l'importance prise par ces services dans la vie économique et sociale, notamment pour ceux qui exercent leur activité en ligne, l'encadrement, tant pour les particuliers que pour les entreprises, du choix et de l'usage des noms de domaine sur internet affecte la liberté de communication et la liberté d'entreprendre. » La référence à la liberté d'entreprendre, qui découle de l'article 4 de la Déclaration de 1789, vient ainsi s'ajouter à la liberté de communication.

Dans la même décision 2010-45 QPC le Conseil constitutionnel reconnait par ailleurs que le législateur doit, conformément à l'article 34 de la Constitution, déterminer « les principes fondamentaux (…) des obligations civiles et commerciales ». Il précise que « ressortissent en particulier aux principes fondamentaux de ces obligations civiles et commerciales les dispositions qui mettent en cause leur existence même ». Il reconnait ainsi une obligation du législateur de fixer des principes généraux pour définir les conditions dans lesquelles les noms de domaine sont attribués ou peuvent être renouvelés, refusés ou retirés.

1.3. CADRE CONVENTIONNEL

Le présent article vise à transposer es mesures issues de l'article 28 la directive 2022/2555 dite NIS 2 en matière d'encadrement de l'enregistrement des noms de domaine. Plus largement, elle s'inscrit dans la stratégie de l'Union européenne pour renforcer la résilience des organisations essentielles au sein de l'Union qui a abouti aux directives n° 2022/2557 dite « REC », concernant la résilience des entités critiques, et n° 2022/2556 dite DORA concernant la résilience opérationnelle numérique du secteur financer.

1.4. ÉLEMENTS DE DROIT COMPARE

Aux Etats-Unis et au Royaume-Uni, l'enregistrement des noms de domaine de premier niveau repose également sur une organisation unique qui reçoit une délégation pour fournir les noms de domaine (*Nominet* au Royaume-Uni et *Neustar* aux Etats-Unis). Les règles d'acquisition sont sensiblement similaires avec une obligation de résidence ou d'exercice d'une activité sur le territoire de l'Etat.

2. NECESSITE DE LEGIFERER ET OBJECTIFS POURSUIVIS

2.1. NECESSITE DE LEGIFERER

Si des dispositions existent dans le droit national, particulièrement dans le CPCE, ces dernières ne permettent pas d'assurer entièrement la transposition des mesures imposées par la directive NIS 2. La transposition des directives est une obligation à valeur constitutionnelle, comme indiqué *supra*, et celle-ci doit être effectuée avant le 17 octobre 2024. La nécessité de légiférer découle donc directement de l'adoption de la directive NIS 2.

2.2. OBJECTIFS POURSUIVIS

L'objectif poursuivi est de mettre en conformité le droit interne avec l'article 28 de la directive NIS 2 concernant l'enregistrement des noms de domaine.

3. OPTIONS POSSIBLES ET DISPOSITIF RETENU

3.1. OPTIONS ENVISAGEES

Aucune autre option n'a été envisagée.

3.2. OPTION RETENUE

La transposition d'une directive étant obligatoire et les mesures modifiées par le présent article étant de nature législative, il est apparu nécessaire de légiférer.

L'article 18 définit les acteurs auxquels les dispositions de la section s'appliquent.

L'article 19 impose à ces acteurs la mise en place d'une base de données.

L'article 20 défini la durée de conservation des données.

L'article 21 impose la publication des données d'enregistrement d'un nom de domaine.

L'article 22 prévoit l'obligation de communiquer ces données à l'autorité judiciaire et à l'autorité nationale de sécurité des systèmes d'information pour les besoins des procédures pénales ou de la sécurité des systèmes d'information.

4. ANALYSE DES IMPACTS DES DISPOSITIONS ENVISAGEES

4.1. IMPACTS JURIDIQUES

4.1.1. Impacts sur l'ordre juridique interne

Les dispositions portées par les articles 19 à 22 ne sont pas codifiée dans le CPCE dans une volonté de ne pas apporter de la confusion entre le dispositif actuel applicable aux enregistrements de nom de domaine et visé aux articles L. 45. L'objet et le champ d'application de ces articles sont différents de celui visé par NIS2.

Au niveau réglementaire, des modifications du décret n° 2015-1317 du 20 octobre 2015 pris en application des articles L. 33-6 et L. 45 du code des postes et des communications électroniques seront nécessaires pour tenir compte des précisions introduites par le présent article aux articles L. 45-4 et L. 45-5 du CPCE.

4.1.2. Articulation avec le droit international et le droit de l'Union européenne

Les modifications prévues par le présent dispositif permettront de se mettre en conformité avec l'article 28 de la Directive NIS 2 qui impose l'obligation de tenu d'une base des données d'enregistrement des noms de domaines, les données collectées et la communication de ces données aux autorités publiques pour des besoins légitimes. Les modifications prévues permettent de rendre l'article pleinement effectif en droit interne.

4.2. IMPACTS ECONOMIQUES ET FINANCIERS

4.2.1. Impacts macroéconomiques

La présente disposition vise à faciliter l'accès à des donnée d'enregistrement exacte par des demandeurs légitimes.

4.2.2. Impacts sur les entreprises

Les offices et les bureaux d'enregistrement devront recueillir les données relatives aux titulaires de noms de domaine et mettre en place des procédures permettant aux services de l'Etat (autorité judiciaire et autorité nationale de sécurité des systèmes d'information) d'accéder à ces données, à leur demande, dans un délai maximal de 72 heures. Le coût de mise en œuvre de ces nouvelles obligations est modeste.

4.2.3. Impacts budgétaires

Il n'y a aucun impact budgétaire notable, dès lors que le dispositif se borne à permettre l'accès des services de l'Etat aux informations relatives aux titulaires de noms de domaine.

4.3. IMPACTS SUR LES COLLECTIVITES TERRITORIALES

Sans objet.

4.4. IMPACTS SUR LES SERVICES ADMINISTRATIFS

Les impacts sur les services administratifs ne sont pas spécifiques à cet article et seront à ce titre identiques à l'ensemble de ceux du projet de loi.

4.5. IMPACTS SOCIAUX

Sans objet.

4.5.1. Impacts sur la société

Sans objet.

4.5.2. Impacts sur les personnes en situation de handicap

Sans objet.

4.5.3. Impacts sur l'égalité entre les femmes et les hommes

Sans objet.

4.5.4. Impacts sur la jeunesse

Sans objet.

4.5.5. Impacts sur les professions réglementées

Sans objet.

4.6. IMPACTS SUR LES PARTICULIERS

La communication des données à un impact sur les données personnelles des particuliers qui aurait recours à des services d'enregistrement de nom de domaine.

4.7. IMPACTS ENVIRONNEMENTAUX

Sans objet.

5. CONSULTATIONS ET MODALITES D'APPLICATION

5.1. CONSULTATIONS MENEES

En application de l'article L. 36-5 du code des postes et des communications électroniques, les présentes dispositions ont été soumises à l'examen de l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse. Le 23 mai 2024, elle a rendu un avis n° 2024-1131 favorable au renforcement des mesures visant à assurer un niveau élevé de cybersécurité. Il appelle à prévoir un délai suffisant aux acteurs pour se mettre en conformité, des critères de désignation des entités suffisamment précis ainsi qu'une bonne articulation de ces nouvelles obligations avec les dispositions du code de la défense pour les opérateurs d'importance vitale.

Conformément aux dispositions de l'article L. 1212-2 du code général des collectivités territoriales, les présentes dispositions ont été soumises à l'examen du Conseil national d'évaluation des normes (CNEN) qui a rendu un avis défavorable le 22 mai 2024.

La Commission supérieure du numérique et des postes a été consultée sur les présentes dispositions. Elle a rendu un avis n° 2024-03 le 21 mai 2024 appelant à s'assurer de la clarté du périmètre des entités concernées et des mesures qu'elles devront appliquer ainsi qu'à mettre en œuvre une stratégie d'accompagnement à la mise en conformité et une politique de supervision progressive.

Sur le fondement de l'article 8 de la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, la Commission nationale de l'informatique et des libertés a été consultée à titre facultatif. Elle a rendu un avis favorable le 23 mai 2024 au renforcement des mesures en matière de cybersécurité, appelant toutefois à s'assurer de la cohérence des exigences de sécurité découlant des principes relatifs à la protection des données avec celles issues de la directive NIS 2 ainsi qu'à une coordination entre la CNIL et l'ANSSI sur la mise en œuvre de NIS 2.

5.2. MODALITES D'APPLICATION

5.2.1. Application dans le temps

Les présentes dispositions entreront en vigueur le lendemain de la publication de la loi au *Journal officiel* de la République française.

5.2.2. Application dans l'espace

L'article est applicable de plein droit dans les départements relevant de l'article 73 de la Constitution (Guadeloupe, Guyane, Martinique, Mayotte, La Réunion).

Il est également applicable dans les collectivités de Saint-Barthélemy, Saint-Martin, Saint-Pierre-et-Miquelon eu égard à leurs lois organiques respectives.

Conformément aux dispositions de l'article 40 du présent projet de loi, le titre II, à l'exception de l'article 13, est applicable dans les îles Wallis et Futuna, en Polynésie française, en Nouvelle-Calédonie et dans les Terres australes et antarctiques françaises, sous réserve des adaptations suivantes :

1° 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 applicables localement.

2° Dans les îles Wallis et Futuna, en Polynésie française et en Nouvelle-Calédonie, les sanctions pécuniaires encourues en vertu du titre II de la présente loi sont prononcées en monnaie locale, compte tenu de la contre-valeur de l'euro dans cette monnaie.

III. – La section 3 du chapitre II du titre II n'est pas applicable en Polynésie française et en Nouvelle-Calédonie.

IV. – Pour l'application du titre II à Saint-Barthélemy, Saint-Pierre-et-Miquelon, dans les îles Wallis et Futuna, en Polynésie française, en Nouvelle-Calédonie et dans les Terres australes et antarctiques françaises, les références à la directive (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 et aux règlements de l'Union européenne sont remplacées par la référence aux règles en vigueur en métropole en vertu de la même directive et des mêmes règlements.

5.2.3. Textes d'application

Un décret en Conseil d'Etat pris après avis CNIL devra définir la liste des données relatives aux noms de domaine devant être collectées ainsi que les modalités d'application concernant la procédure de communication des données à l'autorité judiciaire et à l'autorité nationale de sécurité des systèmes d'information.

Articles 17, 23 et 24 – Notifications d'incidents importants et partage d'informations

1. ÉTAT DES LIEUX

1.1. CADRE GENERAL

L'autorité de sécurité des systèmes d'information en France est l'Agence nationale de la sécurité des systèmes d'information (ANSSI), rattachée au secrétaire général de la défense et de la sécurité nationale (SGDSN). Le ministre de la défense dispose également de compétences spécifiques en matière de cybersécurité prévues par la sous-section 4 de la section 2 du chapitre I^{er} du titre I^{er} du livre IV du code de la défense.

Pour ce qui relève de l'ANSSI, elle assure les fonctions de CERT (*Computer Emergency Response Team*) ou CSIRT (*Computer Security Incident Response Team* – les deux termes, CERT et CSIRT, sont strictement équivalents) national et gouvernemental pour la France. Ces missions de réponse à incident sont exercées au sein du CERT gouvernemental en France, le CERT-FR, créé en 1999, avant la transposition de la directive NIS 1. Le CERT-FR fait partie de l'ANSSI et apporte son appui aux ministères, aux autorités, et à d'autres organismes publics administratifs, ainsi qu'aux opérateurs d'importance vitale (OIV) et opérateurs de services essentiels (OSE).

Le partage d'information et la notification d'incidents et de vulnérabilités font partie des prérogatives du CERT-FR, notamment à travers les missions suivantes :

- détecter les vulnérabilités du système, également grâce à la surveillance de la technologie ;
- aider à la mise en place de moyens de protection contre d'éventuels incidents futurs ;
- gérer les réponses aux incidents, au besoin avec le soutien de partenaires de confiance ;
- favoriser et animer un réseau de confiance, avec différentes entités.

Le CERT-FR fournit des services à la fois réactifs et proactifs, 24h/24 et 7j/7.

- En termes de services réactifs, le CERT-FR assure notamment la réponse aux incidents, l'assistance, le soutien, la remédiation et la rédaction et diffusion des bulletins et alertes relatifs à des vulnérabilités permettant de les corriger.
- En matière de services proactifs, le CERT-FR identifie les vulnérabilités critiques et informe ses bénéficiaires, fournit des services d'audits techniques et d'audits automatisés *via* un portail web, analyse et partage des connaissances sur les menaces,

et partage ces informations dans des enceintes dédiées sur le plan national et international ainsi que via son site web.

De plus, dans le cadre de la coopération et du partage des connaissances, le CERT-FR échange des analyses techniques sur les tactiques, techniques et procédures (TTP) communément utilisées par les attaquants à des fins de prévention et de réaction. Il fait partie de plusieurs groupes de coopération, nationaux comme internationaux, afin d'échanger des informations sur les incidents et les menaces.

L'ANSSI est également destinataire de déclarations d'incidents au titre de plusieurs textes, notamment des opérateurs de services essentiels conformément à la loi n° 2018-133, des opérateurs d'importance vitale concernant leurs systèmes d'information d'importance vitale en vertu de l'article L. 1332-6-2 du code de la défense, des incidents d'origine informatique des opérateurs de communications électroniques en vertu de l'article D. 98-5 du CPCE ou encore des éditeurs de logiciels en vertu de l'article L. 2321-4-1 du code de la défense (non concernés par la directive NIS 2). S'agissant du secret de l'instruction prévu par l'article 11 du code de procédure pénale, qui s'applique par principe, en l'absence de disposition législative contraire, plusieurs textes prescrivent déjà au ministère public de communiquer les suites judiciaires données à une procédure pénale. Une telle obligation figure notamment à l'article 40-2 du code de procédure pénale pour les dénonciations faites par les autorités publiques au titre de l'article 40, le procureur de République devant les aviser des poursuites ou mesures alternatives décidées à la suite de leur signalement. De même, l'article L. 561-30-1 du code monétaire et financier prévoit que, pour les faits susceptibles de relever du blanchiment du produit d'une infraction ou du financement du terrorisme ayant fait l'objet d'une note d'information de la cellule de renseignement financier nationale au procureur de la République, ce dernier doit l'informer de l'engagement d'une procédure judiciaire, du classement sans suite ainsi que des décisions prononcées par les juridictions répressives

Avec la transposition de la directive NIS 2, il est attendu une croissance forte du nombre d'entités régulées. En France, on estime que le nombre d'entités régulées va passer de 500 à près de 15 000. La France a institué, dans cette perspective, une politique de développement de l'écosystème des acteurs de la cybersécurité. Cette politique se traduit par l'accompagnement à la création et la montée en maturité de CSIRT régionaux, sectoriels et ministériels, ainsi qu'une forte collaboration avec le secteur privé pour remplir ces missions, notamment en matière de connaissance de la menace, de notification d'incidents et d'aide à la remédiation.

L'ANSSI a en effet soutenu l'émergence de CSIRT territoriaux, ministériels et sectoriels via le plan France Relance. Douze CSIRT régionaux ont été ouverts en métropole, ainsi que trois centres de ressources cyber ultramarins (Nouvelle-Calédonie, Réunion, Territoires français d'Amériques), étape préliminaire à l'ouverture prochaine de leur CSIRT. En lien avec les politiques économiques des territoires, ces structures offrent un premier niveau

d'accompagnement aux entités de type PME, ETI, collectivités territoriales et associations locales, en assurant les premiers gestes de réponse à incident, en orientant les victimes vers des prestataires et en les coordonnant si nécessaire. Elles les accompagnent aussi dans le dépôt de plainte et les déclarations obligatoires (à la CNIL par exemple) ainsi qu'en matière d'alertes sur les vulnérabilités. Elles conduisent également des missions de prévention vis-à-vis des acteurs sur leurs territoires. Sept CSIRT sectoriels ont également été créés, notamment dédiés aux établissements de santé, à l'enseignement supérieur, au secteur maritime et aux entreprises de défense. Dotés des mêmes capacités que les CSIRT territoriaux, ils se spécialisent dans l'analyse de la menace et des impacts sectoriels aujourd'hui cruciaux pour des organisations à la chaîne d'approvisionnement complexe. Enfin, 10 CSIRT ministériels viennent compléter ce maillage. Ils agissent au profit des administrations centrales des ministères pour leurs systèmes d'information centraux et apportent, en complément du CERT-FR, des services de détection, de réponse à incident et d'analyse de la menace.

L'ANSSI accompagne et contribue à l'InterCERT France, association loi 1901 constituée en novembre 2021, qui vise à renforcer les liens de coopération et à accompagner la montée en maturité des CSIRT français, publics comme privés. De janvier 2022 à juin 2023, l'ANSSI a également assuré au travers du CERT-FR la présidence du CSIRT Network, le réseau des CSIRT à périmètre national de l'Union européenne.

Ces réseaux de CSIRT permettent d'accroître le nombre d'entités en France ayant accès à des capacités de prévention, de détection, de partage d'information et de réaction aux incidents. En tant que CERT gouvernemental, l'ANSSI accompagne le renforcement de la défense du système d'information de l'État via d'autres projets. Elle a par exemple développé, avec la direction interministérielle du numérique (DINUM), des fonctions de cyberdéfense automatisée sur le réseau interministériel de l'État, tout en poursuivant le déploiement de moyens de supervision de la sécurité des systèmes au sein des différents ministères.

1.2. CADRE CONSTITUTIONNEL

Aux termes de l'article 88-1 de la Constitution : « La République participe à l'Union européenne constituée d'Etats qui ont choisi librement d'exercer en commun certaines de leurs compétences en vertu du traité sur l'Union européenne et du traité sur le fonctionnement de l'Union européenne, tels qu'ils résultent du traité signé à Lisbonne le 13 décembre 2007 ». Le Conseil constitutionnel déduit de cette disposition que : « la transposition en droit interne d'une directive communautaire résulte d'une exigence constitutionnelle »[167].Les obligations de notification d'incidents et leurs modalités d'application, tout comme les échanges d'informations entre l'autorité nationale de sécurité des systèmes d'information et d'autres entités, sont susceptibles de porter atteinte au principe de la liberté du commerce et de

[167] CC, décision n° 2004-496 DC du 10 juin 2004, Loi pour la confiance dans l'économie numérique.

l'industrie et notamment à la liberté d'entreprendre, principe à valeur constitutionnelle qui découle de l'article 4 de la Déclaration des droits de l'homme et du citoyen.

La liberté d'entreprendre comprend non seulement la liberté d'accéder à une profession ou à une activité économique mais également la liberté dans l'exercice de cette profession ou de cette activité[168]. Il appartient au législateur d'apporter à cette liberté des limitations liées à des exigences constitutionnelles ou justifiées par l'intérêt général, à la condition qu'il n'en résulte pas d'atteintes disproportionnées au regard de l'objectif poursuivi[169].

Par ailleurs, les présentes dispositions prévoient des obligations de partage d'information relative aux incidents de cybersécurité, notamment vers les partenaires européens, susceptible de conduire à déroger au secret de l'enquête et de l'instruction. Or, le Conseil constitutionnel a pu rappeler que le secret de l'enquête et de l'instruction est une garantie donnée aux citoyens pour assurer à la fois la préservation de l'ordre public en permettant la recherche des auteurs d'infractions, mais aussi une garantie du respect de la présomption d'innocence et de la protection de la vie privée. Il ne peut subir de restriction que si celle-ci est justifiée par un intérêt général et proportionnée à celui-ci[170].

1.3. CADRE CONVENTIONNEL

L'article 11 §3 a) de la directive NIS 2 donne au CSIRT national la tâche de surveiller et analyser les cybermenaces, les vulnérabilités et les incidents au niveau national et, sur demande, d'apporter une assistance aux entités essentielles et importantes concernées pour surveiller en temps réel ou quasi réel leurs réseaux et systèmes d'information.

En matière de notification, NIS 2 prévoit, à son article 23, un mécanisme échelonné pour la notification des incidents[171] importants pour les entités essentielles et importantes. En matière de notification d'incidents significatifs, la directive NIS 2 établit plusieurs étapes afin de trouver le juste équilibre entre « la notification rapide qui aide à atténuer la propagation potentielle des incidents importants et permet aux entités essentielles et importantes de chercher de l'aide » et la « notification approfondie qui permet de tirer des leçons précieuses des incidents individuels et d'améliorer au fil du temps la cyber résilience des entreprises individuelles et de secteurs tout entiers ». Cela comprend :

---

[168] Conseil constitutionnel, Décision n° 2012-285 QPC, 30 novembre 2012.

[169] Conseil constitutionnel, décision n° 2000-429 DC, 30 mai 2000.

[170] Conseil constitutionnel, décision n° 2017-693 QPC du 2 mars 2018.

[171] L'incident est défini dans la directive NIS 2 comme un événement compromettant la disponibilité, l'authenticité, l'intégrité ou la confidentialité des données stockées, transmises ou faisant l'objet d'un traitement, ou des services que les réseaux et systèmes d'information offrent ou rendent accessibles.

- Une « alerte précoce », sous un délai de 24h après avoir eu connaissance de l'incident important, qui le cas échéant indique si l'on suspecte que l'incident important a été causé par des actes illicites ou malveillants ou s'il pourrait y avoir un impact transfrontière ;
- Une « notification d'incident », sous un délai de 72h après avoir eu connaissance de l'incident important, qui le cas échéant met à jour les informations fournies au titre de l'alerte précoce, et fournit une évaluation initiale de l'incident, y compris sa gravité et son impact, et les indicateurs de compromission quand disponibles ;
- A la demande du CSIRT, un « rapport intermédiaire » sur les mises à jour pertinentes de la situation ;
- Un « rapport final », dans un délai d'un mois, sous réserve que l'incident soit traité, dont le contenu est précisé à l'article 23, paragraphe 4, point d ;
- Dans le cas contraire, un « rapport d'avancement », dans un délai d'un mois, devant être complété par un rapport final dans un délai d'un mois après le traitement de l'incident.

La directive NIS 2 prévoit également, à son article 23, paragraphe 1 et 2 de la directive NIS 2, que les entités notifient le cas échéant, et sans retard injustifié, aux destinataires de leurs services les incidents importants susceptibles de nuire à la fourniture de ces services et qu'elles communiquent avec ceux affectés par une cybermenace importante, toutes les mesures ou corrections que ces destinataires peuvent appliquer en réponse à cette menace. Une cybermenace importante est « une cybermenace qui, compte tenu de ses caractéristiques techniques, peut être considérée comme susceptible d'avoir un impact grave sur les réseaux et les systèmes d'information d'une entité ou les utilisateurs des services de l'entité, en causant un dommage matériel, corporel ou moral considérable ».

Enfin, l'article 23, paragraphe 7 de la directive NIS 2, prévoit, entre autres mesures, que le CSIRT puisse imposer aux entités d'informer le public de l'incident important, lorsque la sensibilisation du public est nécessaire pour prévenir ou faire face à un incident important, ou lorsque la divulgation de l'incident est dans l'intérêt public.

En matière de partage d'informations, l'article 29 de la directive prévoit que les Etats membres veillent à ce que les entités importantes et les entités essentielles s'organisent pour échanger des informations cyber entre elles. Par ailleurs, l'article 10 paragraphe 3 de la directive prévoit que chaque CSIRT national dispose d'une infrastructure de communication et d'information adaptée, sécurisée et résiliente, permettant d'échanger des informations avec les entités et les autres parties prenantes, incluant la contribution au déploiement d'outils sécurisés de partage d'informations.

1.4. ELEMENT DE DROIT COMPARE

La Belgique a souhaité inscrire dans son projet de loi de transposition de NIS 2 les différentes étapes et obligations fixées par la directive en matière de notification d'incidents significatifs. Comme cela est envisagé au niveau français, le texte renvoie ensuite au niveau règlementaire la définition des seuils précis de notification en fonction du degré d'impact ou d'urgence de l'incident.

2. NECESSITE DE LEGIFERER ET OBJECTIFS POURSUIVIS

2.1. OBJECTIFS POURSUIVIS

Notification d'incidents

Pour rappel, la directive NIS 2 établit des obligations de notification d'incidents[172] pour les entités essentielles et importantes. La notification à l'autorité nationale doit être distinguée de l'information des utilisateurs, qui n'intervient que dans un second temps et en tant que de besoin.

Les objectifs poursuivis dans ce cadre sont de plusieurs ordres sur le plan opérationnel :

- renforcer le rôle du CERT-FR et les obligations des entités essentielles et importantes en termes de notification d'incidents ;
- maintenir une cohérence avec le dispositif existant en matière de terminologie ;
- obliger toutes les victimes d'un incident critique ou susceptible de nuire à la fourniture de ces services ou d'une vulnérabilité[173] critique affectant les réseaux et les systèmes d'information, à informer leurs clients, à l'exception des informations dont la divulgation porterait atteinte aux intérêts de la défense ou de la sécurité nationale ;
- améliorer la communication des informations sur les incidents transfrontières et trans sectoriels à l'autorité nationale par les entités ;
- prévoir un pouvoir d'injonction de l'autorité nationale pour que les entités informent et signalent leurs incidents aux victimes ou publiquement.

Partage d'informations

Les objectifs opérationnels liés au partage d'informations sont de plusieurs ordres :

[172] L'incident est défini dans la directive comme un événement compromettant la disponibilité, l'authenticité, l'intégrité ou la confidentialité des données stockées, transmises ou faisant l'objet d'un traitement, ou des services que les réseaux et systèmes d'information offrent ou rendent accessibles.

[173] La vulnérabilité est définie dans la directive comme une faiblesse, susceptibilité ou une faille de produits TIC ou de services TIC qui peut être exploitée par une cybermenace.

- divulgation coordonnée de vulnérabilités : le signalement de vulnérabilité doit pouvoir être réalisé de manière anonyme, à la demande de son émetteur. Cette disposition n'appelle pas de marge d'appréciation et ne fait pas l'objet de besoin métier. En revanche, un point d'attention est identifié sur la nécessité de ne pas prévoir de disposition qui serait ensuite remise en cause par les dispositions du futur règlement européen *Cyber Resilience Act* (CRA) ;
- partage d'information et coopération avec le secteur privé ;
- mise à disposition d'outils de partage ;
- si l'incident touche deux Etats membres, prévoir la possibilité, par défaut, de partager certaines informations sur les incidents signalés : il est souhaité que les données contextuelles techniques d'un incident signalé au CERT-FR puissent être partagées pour répondre aux besoins de coopération, sauf si la victime ou la sensibilité du sujet (ex. affaire judiciarisée ou informations classifiées) s'y oppose ;
- transmission d'informations dans le cadre de l'évaluation par les pairs en présence d'observateurs : les informations échangées se limitent au minimum nécessaire et sont proportionnées à l'objectif de cet échange.

Les objectifs poursuivis dans le cadre de la transposition de cette mesure sont les suivants :

- Être destinataire de toutes les notifications d'incidents dans les meilleurs délais, au titre de l'article 11 §3 a) de la directive ;
- En tant que CSIRT gouvernemental et national, assurer la diffusion de l'information aux bons relais au bon moment.

2.2. NECESSITE DE LEGIFERER

Aux termes de l'article 88-1 de la Constitution : « La République participe aux Communautés européennes et à l'Union européenne, constituées d'Etats qui ont choisi librement, en vertu des traités qui les ont instituées, d'exercer en commun certaines de leurs compétences ». Le Conseil constitutionnel déduit de cette disposition que « la transposition en droit interne d'une directive communautaire résulte d'une exigence constitutionnelle »[174].

Notification d'incidents

L'article 17 du projet de loi doit être adopté au niveau législatif, eu égard à ses conséquences sur l'activité des entités. Cette disposition vient en effet imposer des obligations de

[174] Voir notamment la décision n° 2004-496 DC du 10 juin 2004, « Loi pour la confiance dans l'économie numérique ».

notification d'incidents, la nature des incidents qui doivent être notifiés et les destinataires de ces notifications.

Des dispositions législatives sont donc nécessaires pour définir un cadre et apporter des garanties suffisantes afin d'éviter les atteintes disproportionnées à la liberté du commerce et de l'industrie, liberté publique au sens de l'article 34 de la Constitution, et à la liberté d'entreprendre, découlant de l'article 4 de la Déclaration des droits de l'homme et du citoyen de 1789.

Partage d'informations

L'article 23 du projet de loi doit être adopté au niveau législatif, eu égard à ses conséquences sur les secrets protégés par la loi et la sécurité nationale.

Ces dispositions peuvent également impliquer la communication d'informations relevant du secret des affaires, dont la protection est fondée sur les articles L. 151-1 et suivants du code de commerce. L'article L. 151-1 du code de commerce définit la notion d'information protégée au titre du secret des affaires selon trois critères : cette information n'est pas généralement connue ou aisément accessible pour les personnes familières de ce type d'informations ; elle revêt une valeur commerciale, effective ou potentielle, du fait de son caractère secret ; elle fait l'objet de la part de son détenteur légitime de mesures de protection raisonnables, pour en conserver le caractère secret.

Bien que les articles L. 151-7 à L. 151-9 du code de commerce prévoient des exceptions au secret des affaires, ces exceptions ne couvrent pas l'échange d'informations entre les entités mentionnées à l'article 23 du projet de loi.

En outre, les informations échangées peuvent contenir des données à caractère personnel.

Enfin, l'échange d'information impose de prévoir une dérogation au secret professionnel, auquel sont astreints les agents publics, en application de l'article L. 121-6 du code général de la fonction publique.

Une disposition législative est donc nécessaire pour, d'une part, définir un cadre et apporter des garanties suffisantes à la sécurité nationale, la sécurité publique ou la défense nationale et, d'autre part, déroger aux secrets protégés par la loi et au secret de l'instruction.

L'article 24 du projet de loi doit être adopté au niveau législatif, eu égard à ses conséquences sur des organismes privés agréés par l'autorité nationale de sécurité des systèmes d'information. Cette disposition prévoit en effet des obligations de diffusion d'alertes et d'informations et de coopération avec l'autorité nationale de sécurité des systèmes d'information.

Une disposition législative est donc nécessaire pour définir un cadre et apporter des garanties suffisantes afin d'éviter les atteintes disproportionnées à la liberté du commerce et de l'industrie et à la liberté d'entreprendre.

Par ailleurs, les dispositions concernant les collectivités territoriales, leurs groupements et établissements publics locaux en tant qu'entités essentielles ou importantes doivent être adoptées au niveau législatif.

3. OPTIONS ENVISAGEES ET DISPOSITIF RETENU

3.1. OPTIONS ENVISAGEES

Sans objet.

3.2. DISPOSITIF RETENU

Notifications d'incidents majeurs

Les entités essentielles et importantes notifient, sans retard injustifié par rapport aux différents délais fixés par la directive, à l'autorité nationale de sécurité des systèmes d'information tout incident ayant un impact important sur la fourniture de leurs services. Dans certains cas prévus par la loi (prévenir un incident concernant une entité essentielle ou une entité importante ou faire face à un incident en cours, ou lorsque la divulgation de l'incident est dans l'intérêt public), l'autorité nationale de sécurité des systèmes d'information peut, après avoir consulté l'entité essentielle ou importante concernée, exiger de l'entité qu'elle informe le public de l'incident ou le faire elle-même.

Afin de ne pas obliger la notification de tout incident, mais bien de se limiter aux incidents significatifs, des critères d'évaluation d'impacts ou de seuils permettant de caractériser un tel incident dans le cadre de la directive NIS 2 seront précisés au niveau règlementaire sur une base similaire à ce qui a été fait pour la loi de programmation militaire (LPM) pour 2024-2030. Une définition du caractère significatif d'un incident de cybersécurité y a en effet déjà été intégrée. Cette définition est une déclinaison de la notion telle qu'établie à l'article 20 3 b de la directive NIS 2 ("*the incident has affected or has the potential to affect other natural or legal persons by causing considerable material or non-material losses*.") mais adaptée au contexte d'un produit numérique. La liste de critères pour les vulnérabilités significatives et les incidents compromettant la sécurité d'un système d'information sera précisée par décret.

Les entités essentielles et importantes notifient, sans délai, aux destinataires de leurs services, à l'exception des informations dont la divulgation porterait atteinte aux intérêts de la défense ou de la sécurité nationale :

- les incidents critiques susceptibles de nuire à la fourniture de ces services ;
- les vulnérabilités critiques affectant leurs services ou les affectant potentiellement, ainsi que les mesures ou corrections, dès qu'elles en ont connaissance, que ces destinataires peuvent appliquer en réponse à cette vulnérabilité ou à cette menace.

L'autorité nationale de sécurité des systèmes d'information recueille la liste des destinataires des services des entités essentielles et importantes concernées, qui peuvent la lui communiquer en cas d'incident critique ou de vulnérabilité critique. Elle tient compte 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.

A noter que l'obligation de notification positionne l'autorité nationale comme centralisateur des éléments afin de mieux orienter ses capteurs de veille au niveau national, et donc mieux anticiper la menace à laquelle la France est confrontée. Cette position lui permet de réduire le risque de dilution de l'information en matière de menace comme d'incidentologie et de mieux partager l'information auprès des écosystèmes de CSIRT relais sur le plan national.

Les modalités d'application de cette disposition seront fixées par décret en Conseil d'Etat.

Partage d'informations

L'article 23 du projet de loi prévoit une obligation de coopération de l'autorité nationale de sécurité des systèmes d'information avec la Commission nationale de l'informatique et des libertés, les autorités compétentes en charge de la gestion des risques en matière de cybersécurité en vertu d'un acte sectoriel de l'Union, les autorités chargées de la conduite de la politique pénale, de l'action publique et de l'instruction, ainsi que les organismes internationaux concourant aux missions de sécurité ou de défense des systèmes d'information. L'autorité nationale de sécurité des systèmes d'information peut également communiquer aux organismes internationaux concourant aux missions de sécurité ou de défense des systèmes d'information, sur leur demande ou à son initiative, les informations qu'elle détient sur les incidents informatiques. L'autorité nationale de sécurité des systèmes d'information coopère avec la Commission européenne et les autorités compétentes des autres Etats membres de l'Union européenne. Elle peut également coopérer avec des centres de réponse aux incidents de sécurité informatique ou des organismes équivalents des Etats tiers à l'Union européenne. L'autorité nationale de sécurité des systèmes d'information coopère avec la Commission européenne et les autorités compétentes des autres Etats membres de l'Union européenne. Elle peut également coopérer avec des centres de réponse aux incidents de sécurité informatique ou des organismes équivalents des Etats tiers à l'Union européenne.

Ces entités peuvent se communiquer librement les informations dont elles disposent et se consulter mutuellement aux fins de l'accomplissement de leurs missions respectives, à l'exception des informations dont la communication porterait atteinte à la sécurité publique, à la défense et la sécurité nationale ou à la conduite des relations internationales.

Pour certains de ces organismes, l'article 23 prévoit une dérogation aux secrets protégés par la loi et au secret de l'instruction. Pour l'ensemble des organismes avec lesquels l'autorité nationale est tenue de coopérer, des données à caractère personnel sont susceptibles d'être communiquées. Par ailleurs, l'autorité nationale ne peut pas communiquer des informations qui porteraient atteinte à la sécurité nationale, la sécurité publique ou la défense nationale. Cela exclut donc la communication d'informations couvertes par le secret de la défense nationale.

L'article 23 ne liste pas l'intégralité des secrets protégés par la loi auxquels sont apportés une dérogation mais mentionne les « autres secrets protégés par la loi ». Cette formulation est liée au risque d'enchevêtrement des secrets protégés par la loi applicables à une même information partagée entre les différentes entités listées par l'article en question. Or, l'article 2 §13 de la directive n° 2022/2555 prévoit une dérogation aux secrets protégés par la législation nationale dès lors que l'échange de ces informations est nécessaire à l'application de la directive. Tous les secrets protégés par la loi sont donc concernés. De plus, la formulation mentionnant les « autres secrets protégés par la loi » existe déjà au niveau législatif, à l'article L. 311-5 du code des relations entre le public et l'administration : « 2° Les autres documents administratifs dont la consultation ou la communication porterait atteinte : […] h) Ou sous réserve de l'article L. 124-4 du code de l'environnement, aux autres secrets protégés par la loi ».

Il a été décidé de ne pas rendre obligatoire les outils de partage qui seront mis à disposition, notamment pour limiter le coût à la charge des entités nouvellement régulées.

L'article 24 prévoit les missions des organismes publics ou privés agréés par l'autorité nationale des systèmes d'information et autorise les échanges d'informations couvertes par des secrets protégés par la loi.

4. ANALYSE DES IMPACTS DES DISPOSITIONS ENVISAGEES

4.1. IMPACTS JURIDIQUES

4.1.1. Impacts sur l'ordre juridique interne

Notification d'incident

L'article 17 du présent projet de loi créent de nouvelles dispositions qui ne seront pas codifiées. Il prévoit les obligations et délais de notification d'incident à l'autorité nationale de sécurité des systèmes d'information et aux destinataires des services des entités concernées. Il prévoit également les obligations d'information du public de certains incidents.

Partage d'informations

Les articles 23 sur les modalités de la coopération de l'autorité nationale de sécurité des systèmes d'information avec d'autres entités nationales, européennes et internationales, ainsi que 24 relatif aux missions des organismes publics ou privés agréés, du présent projet de loi créent de nouvelles dispositions qui ne seront pas codifiées.

A noter que la coopération entre l'autorité nationale de sécurité des systèmes d'information et les autorités chargées de la conduite de la politique pénale, de l'action publique et de l'instruction est justifiée par la lutte contre la cybercriminalité. La dérogation faite au secret de l'enquête et de l'instruction est proportionnée, dans la mesure où l'échange d'information demeure une faculté et non une obligation faite à l'autorité judiciaire.

4.1.2. Articulation avec le droit international et le droit de l'Union européenne

La directive NIS 2 mentionne à plusieurs reprises la possibilité d'échanger des données, y compris des données à caractère personnel avec des pays situés hors de l'Union européenne. En revanche, le Règlement général sur la protection des données reste applicable et ces partages d'information doivent notamment s'inscrire dans le cadre des mécanismes de protection des données tels que les décisions d'adéquation.

A titre d'exemple, à l'article 11, il est prévu que :

« *7. Les CSIRT peuvent établir des relations de coopération avec les centres de réponse aux incidents de sécurité informatique nationaux de pays tiers. Dans le cadre de ces relations de coopération, les États membres facilitent un échange d'informations effectif, efficace et sécurisé avec ces centres de réponse aux incidents de sécurité informatique nationaux de pays tiers, en utilisant les protocoles d'échange d'informations appropriés, y compris le « Traffic Light Protocol ». Les CSIRT peuvent échanger des informations pertinentes avec des centres de réponse aux incidents de sécurité informatique nationaux de pays tiers, y compris des données à caractère personnel, dans le respect du droit de l'Union en matière de protection des données.*

8. Les CSIRT peuvent coopérer avec des centres de réponse aux incidents de sécurité informatique nationaux de pays tiers ou des organismes équivalents de pays tiers, notamment dans le but de leur fournir une assistance en matière de cybersécurité ».

Cet article est éclairé par le considérant 45 qui précise que « *Compte tenu de l'importance de la coopération internationale en matière de cybersécurité, les CSIRT devraient pouvoir participer à des réseaux de coopération internationaux en plus du réseau des CSIRT institué par la présente directive. Par conséquent, aux fins de l'accomplissement de leurs tâches, les CSIRT et les autorités compétentes devraient pouvoir échanger des informations, y compris des données à caractère personnel, avec les centres de réponses aux incidents de sécurité informatique nationaux ou les autorités compétentes de pays tiers, pour autant que les conditions prévues par le droit de l'Union en matière de protection des données pour les*

transferts de données à caractère personnel vers des pays tiers, entre autres celles de l'article 49 du règlement (UE) 2016/679, soient remplies ».

De la même manière, le considérant 74 prévoit que « *Afin de faciliter la mise en œuvre effective de la présente directive, entre autres en ce qui concerne la gestion des vulnérabilités, les mesures de gestion des risques en matière de cybersécurité, les obligations d'information et les accords de partage d'informations en matière de cybersécurité, les États membres peuvent coopérer avec des pays tiers et entreprendre des activités jugées appropriées à cette fin, y compris des échanges d'informations sur les cybermenaces, les incidents, les vulnérabilités, les outils et méthodes, les tactiques, les techniques et les procédures, la préparation et les exercices pour la gestion des crises de cybersécurité, la formation, le renforcement de la confiance ainsi que les arrangements permettant de partager les informations de façon structurée* ».

A cette fin, l'article 23 du projet de loi prévoit la possibilité d'échanger des informations avec diverses entités aux fins de l'accomplissement de leurs missions respectives sous réserve de la préservation 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.

4.2. IMPACTS ECONOMIQUES ET FINANCIERS

4.2.1. Impacts macro-économiques

L'ANSSI dispose d'un panorama de la menace cyber qui lui permet d'objectiver le risque cyber et les impacts potentiels d'une menace ou information. Grâce à son positionnement, le CERT-FR est en mesure de mieux prévoir et prendre en compte l'exposition aux risques et ainsi d'évaluer la pertinence ou non de partager l'information. Tout partage d'informations est en effet évalué au regard du risque, l'information portant sur une valeur, une criticité, un coût qui évoluent au cours de son cycle de vie. La gouvernance de l'information est donc un enjeu clé qui doit être porté avec responsabilité particulièrement au regard de l'effet systémique potentiel du risque cyber. Dans ce cadre, on peut considérer que l'effet de cette mesure peut être important sur le plan macro-économique dès lors qu'il peut réduire un risque d'exploitation de faille, de compromission, propre à nuire aux intérêts économiques de la Nation.

Aujourd'hui, le contexte économique laisse apparaître certaines tendances en matière de menaces économiques. L'analyse de ces menaces montre de plus en plus une sophistication et une simultanéité des attaques opérées par des acteurs ingérants.

Pour répondre à l'augmentation de la menace avec des acteurs malveillants toujours plus performants et mieux outillés, touchant de plus en plus d'entités trop souvent mal protégées, l'autorité nationale de sécurité des systèmes d'information doit pouvoir renforcer sa capacité

opérationnelle, dans un contexte où la transposition de la directive va élargir son périmètre d'activité dans une mesure sans précédent en matière de réglementation cyber. En France, cela se traduit effectivement par une augmentation estimée du nombre d'entités régulées de 500 à près de 15 000, et une augmentation du nombre de secteurs régulés de 6 à 18.

Ainsi, pour répondre aux obligations de partage de l'information et renforcer les capacités de cyberdéfense de la Nation, l'ANSSI travaille depuis plusieurs années au développement de l'écosystème de partenaires privés. A ce titre, l'émergence d'une stratégie nationale de prévention et d'assistance aux victimes de cybermalveillance, en lien avec le secteur privé à travers le Groupement d'intérêt public *Action contre la cybermalveillance* (GIP Acyma), la densification du réseau de centres de réponse aux incidents cyber (CSIRT ministériels, régionaux et sectoriels) ou encore la mobilisation des Campus Cyber pour renforcer le lien nécessaire entre acteurs privés et acteurs publics, participent au maillage territorial et sectoriel des dispositifs, au plus près des besoins opérationnels. Le développement de cet écosystème cyber de confiance constitue un levier de croissance et de montée en compétences cyber. Son impact économique et en termes d'image de la France dans la sphère cyber internationale est à considérer de manière directe et indirecte.

4.2.2. Impacts sur les entreprises

Cette mesure, renforcée par le partage entre Etats membres, peut contribuer à renforcer la cyber-protection des entités européennes d'intérêt. Ses effets directs et indirects pourraient être importants tant sur le plan de la sécurité que sur la croissance des entités essentielles et importantes, dès lors qu'elles sauront s'approprier et mettre à profit les recommandations et les mesures de remédiation, notamment en matière de vulnérabilités.

En ce qui concerne l'agrément d'organismes publics et privés en tant que relais dans la prévention et la gestion des incidents, la structuration d'un réseau de CSIRT relais aura deux impacts principaux : le développement au niveau régional d'une filière cyber, via la valorisation de prestataires de confiance auprès de clients potentiels, et le renforcement de l'attractivité des territoires où la présence de prestataires cyber de proximité deviendra une garantie de sécurité pour les acteurs économiques.

4.2.3. Impacts budgétaires

Concernant la seule mise en œuvre des obligations de notification et de partage de l'information, la charge budgétaire pesant sur les administrations en général apparaît mesurée voire nulle, car de telles notifications sont déjà effectuées vers l'autorité nationale de sécurité des systèmes d'information.

Pour l'ANSSI, cette mesure aura pour effet principal de renforcer les capacités de supervision de l'ANSSI, sans engendrer en tant que telle d'impact significatif sur ses moyens (qui devront

en revanche être adaptés à l'extension de son champ de compétence découlant des autres dispositions du projet de loi).

4.3. IMPACTS SUR LES COLLECTIVITES TERRITORIALES

Il n'y a pas d'impact particulier de cette mesure sur les collectivités territoriales. Il convient cependant de noter que dans le cas particulier des régions, cette mesure implique qu'elles maintiennent en état de fonctionnement leurs CSIRT régionaux, actuellement au nombre de douze (toutes les régions de l'hexagone, hors Auvergne-Rhône-Alpes, ainsi que trois Centres de ressources cyber ultramarins en Nouvelle-Calédonie, à la Réunion et dans les territoires français d'Amériques qui travaillent eux-mêmes à l'ouverture prochaine de leurs centres de réponse à incident), sans qu'elle ne crée de charge additionnelle particulière.

En effet, un partage d'informations est déjà organisé régulièrement entre le CERT-FR et les CSIRT régionaux via des points de situation bilatéraux organisés tous les quinze jours. Ces points sont l'occasion pour le CERT-FR de capter des informations relatives à des cybermenaces en région et donc des opportunités pour détecter les signaux faibles précurseurs d'attaques de grande ampleur ou susceptibles de viser des entités critiques. Réciproquement, ces échanges permettent au CERT-FR d'informer les CSIRT de signalements qui lui sont remontés et qui impactent leurs bénéficiaires, voire, si la maturité d'un CSIRT le permet, d'envisager des désescalades d'incidents vers le CSIRT. Au-delà du bénéfice opérationnel de ces échanges, ces derniers permettent de développer la coopération entre le CERT-FR et les CSIRT, ainsi que d'éprouver la fiabilité des processus de traitement coordonné d'un incident.

4.4. IMPACTS SUR LES SERVICES ADMINISTRATIFS

Au niveau des administrations publiques nationales, les dernières évaluations du niveau de cybersécurité en date montrent un certain retard de ce secteur par rapport au secteur privé. Il conviendrait par conséquent, pour s'assurer que ces entités puissent atteindre la conformité à la directive NIS 2, qu'une part plus substantielle de leurs budgets numériques soient consacrés à la sécurité numérique. L'effort adapté est estimé à 5% des budgets numériques des ministères. Certains ministères consacrent déjà de tels moyens à leur sécurité numérique, tandis qu'un rééquilibrage limité devra être réalisé par d'autres pour se mettre en conformité. Des emplois publics seront également consacrés aux CSIRT ministériels relais.

Concernant l'impact de cette mesure sur l'ANSSI, compte-tenu de l'extension du périmètre d'application de la directive NIS 2, on peut envisager qu'il y aura davantage de transmissions de signalements d'incidents vers l'autorité nationale. La sous-direction Opérations s'est réorganisée pour pouvoir assurer les missions qui seront les siennes. Ainsi, une nouvelle Division Écosystèmes, services et coopération (DESC) a été créée afin de coordonner la fourniture vers l'extérieur des services portés par la sous-direction Opérations sous la

« marque » CERT-FR. Elle assure de manière cohérente et massive, en appui de l'expertise métier nécessaire, la délivrance des services permettant de démultiplier les actions de prévention, protection et résilience auprès de l'ensemble de ses bénéficiaires directs et indirects de l'autorité nationale comme le prévoit la directive NIS 2. Le dispositif proposé nécessite donc la création de 14 emplois dans cette mission de recueil des signalements et de relations opérationnelles avec les entités régulées, pour un total de 32 postes d'ici à 2027.

Par ailleurs, pour assurer le service auprès d'un nombre d'acteurs démultiplié, le CERT-FR devra bâtir les outils nécessaires à son efficacité : les outils de coopération et partenariats et les outils nécessaires à la bonne gestion des relations avec les organismes agréés.

4.5. IMPACTS SOCIAUX

4.5.1. Impacts sur la société

La transposition de la directive NIS 2 crée de nouvelles obligations sur un grand nombre d'activités au sein de l'UE, ce qui nécessite de mobiliser de nombreuses compétences en cybersécurité, allant des plus techniques, comme les tests de pénétration de réseaux ou les investigations suite à incident, à celles relatives à la gouvernance, comme la gestion de crise, ou à des connaissances méthodologiques, comme les analyses de risque.

La consécration dans le texte de transposition de l'obligation de notification des incidents et du partage d'informations constitue, de la même manière, une opportunité de création d'emplois, dont on sait qu'ils seront pérennes à la fois chez les entités régulées privées, au sein des administrations et dans les équipes des prestataires de services en cybersécurité, de plus en plus sollicités.

4.5.2. Impacts sur les personnes en situation de handicap

Sans objet.

4.5.3. Impacts sur l'égalité entre les femmes et les hommes

Sans objet.

4.5.4. Impacts sur la jeunesse

Sans objet.

4.5.5. Impacts sur les professions réglementées

Sans objet.

4.6. IMPACT ENVIRONNEMENTAL

On peut envisager un impact positif concernant le coût carbone dans la mesure où les entités disposeront de compétences propres en interne, ce qui limitera les cas de nécessité de déplacements sur site pour les différents prestataires et parties prenantes aux missions de réponse à incident.

5. CONSULTATIONS ET MODALITES D'APPLICATION

5.1. CONSULTATIONS MENEES

Un travail a été mené depuis plusieurs années pour bâtir un écosystème relais de confiance : CSIRT ministériels, sectoriels ou territoriaux ou prestataires qualifiés, avec lesquels l'ANSSI échange régulièrement.

Conformément aux dispositions de l'article L. 1212-2 du code général des collectivités territoriales, les présentes dispositions ont été soumises à l'examen du Conseil national d'évaluation des normes (CNEN) qui a rendu un avis défavorable le 22 mai 2024.

La Commission supérieure du numérique et des postes (CSNP) a été consultée sur les présentes dispositions. Elle a rendu un avis n° 2024-03 le 21 mai 2024 appelant à s'assurer de la clarté du périmètre des entités concernées et des mesures qu'elles devront appliquer ainsi qu'à mettre en œuvre une stratégie d'accompagnement à la mise en conformité et une politique de supervision progressive.

Sur le fondement de l'article 8 de la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, la Commission nationale de l'informatique et des libertés a été consultée à titre facultatif. Elle a rendu un avis favorable le 23 mai 2024 au renforcement des mesures en matière de cybersécurité, appelant toutefois à s'assurer de la cohérence des exigences de sécurité découlant des principes relatifs à la protection des données avec celles issues de la directive NIS 2 ainsi qu'à une coordination entre la CNIL et l'ANSSI sur la mise en œuvre de NIS 2.

5.2. MODALITES D'APPLICATION

5.2.1. Application dans le temps

Les présentes dispositions entreront en vigueur le lendemain de la publication de la loi au *Journal officiel* de la République française.

5.2.2. Application dans l'espace

Conformément à l'article 40 du présent projet de loi, le titre II, à l'exception de l'article 13, est applicable dans les îles Wallis et Futuna, en Polynésie française, en Nouvelle-Calédonie et dans les Terres australes et antarctiques françaises, sous réserve des adaptations suivantes :

1° 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 applicables localement.

2° Dans les îles Wallis et Futuna, en Polynésie française et en Nouvelle-Calédonie, les sanctions pécuniaires encourues en vertu du titre II de la présente loi sont prononcées en monnaie locale, compte tenu de la contre-valeur de l'euro dans cette monnaie.

Pour l'application du titre II à Saint-Barthélemy, Saint-Pierre-et-Miquelon, dans les îles Wallis et Futuna, en Polynésie française, en Nouvelle-Calédonie et dans les Terres australes et antarctiques françaises, les références à la directive (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 et aux règlements de l'Union européenne sont remplacées par la référence aux règles en vigueur en métropole en vertu de la même directive et des mêmes règlements.

5.2.3. Textes d'application

Un décret en Conseil d'Etat fixe les modalités d'application de la notification obligatoire des incidents majeurs. Il précise notamment la procédure applicable et les critères d'appréciation des caractères importants et critiques des incidents et vulnérabilités ainsi que les délais de notification des incidents et des vulnérabilités.

Un décret en Conseil d'Etat précise également le partage d'information nécessaire à l'accomplissement des missions de l'autorité nationale de sécurité des systèmes d'information d'une part et de certains organismes d'autre part ainsi que les modalités de dépôt et d'examen des demandes d'agrément des organismes agréés par l'autorité nationale de sécurité des systèmes d'information.

CHAPITRE III – DE LA SUPERVISION

Articles 25 à 37 – Supervision – Procédures de contrôle et de sanction

1. ETAT DES LIEUX

1.1. CADRE GENERAL

Différentes dispositions en matière de cybersécurité, issues pour certaines du droit européen, prévoient des dispositifs de supervision se traduisant notamment par des mécanismes de contrôle et de sanction en cas de manquement aux règles qu'elles instaurent vis-à-vis des opérateurs relevant de leur champ d'application.

L'ANSSI, en tant qu'autorité nationale en matière de sécurité des systèmes d'information, a été désignée comme l'autorité en charge de faire appliquer ces dispositions. Au titre du dispositif SIIV[175], présenté *supra* à l'article 1er, et de la loi[176] transposant 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 (directive « NIS 1 »), l'autorité nationale de sécurité des systèmes d'information (ANSSI) est en charge de faire appliquer par les opérateurs régulés un ensemble d'exigences relatives à la cybersécurité de leurs systèmes d'information d'importance vitale ou essentiels.

Des régimes de sanctions pénales, prenant la forme d'amendes, sont d'ores et déjà en vigueur[177] et sont destinés à inciter les opérateurs à se mettre en conformité avec les règles de déclaration, de gestion des risques et des incidents, ainsi qu'à un ensemble d'exigences techniques, sur la partie de leur activité qui repose de manière critique sur des moyens numériques. Ces sanctions sont applicables aux manquements de la part des opérateurs factuellement constatés concernant, notamment : le non-respect des règles de sécurité numérique fixées par le Premier ministre, l'obligation de déclaration des incidents de sécurité ou d'information du public, le déroulement des contrôles commandés par le Premier ministre. Toutefois, il est apparu que les mécanismes de sanction étaient peu adaptés, n'offrant par

[175] Articles L. 1332-6-1 à L. 1332-7, et R. 1332-41-1 à R. 1332-41-23 et R. 1332-42 du code de la défense.

[176] 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.

[177] Article L. 1332-7 du code de la défense et articles 9 et 15 de la loi n°2018-133 du 26 février 2018.

exemple pas la possibilité d'une approche graduée par l'autorité nationale de sécurité des systèmes d'information. Ils n'ont, de fait, jamais été mis en œuvre.

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 « NIS 2 ») prévoit à son article 36 l'instauration d'un régime de sanctions administratives, parallèlement à l'élargissement du champ d'application des exigences, engendrant une forte augmentation du nombre des entités régulées, et par conséquent une forte augmentation du nombre d'opérateurs pour lesquels des sanctions administratives sont susceptibles d'être prononcées en cas de manquement.

Par ailleurs, au titre du règlement eIDAS de 2014[178], 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 : organe de contrôle des prestataires de confiance, organisme de certification des dispositifs de création de signature et cachet électronique qualifiés (QSCD), organisme chargé d'établir, tenir à jour et publier la liste nationale de confiance. La mission de vérification du respect des exigences de sécurité pour les moyens d'identification électronique relevant d'un schéma notifié par la France lui échoit également. Outre les pouvoirs de contrôle conférés à l'ANSSI, un régime national prévoyant des sanctions effectives, proportionnées et dissuasives doit être instauré.

En outre, au titre du règlement *Cyber Security Act* (CSA) de 2019[179], qui prévoit une gouvernance européenne pour adopter des schémas de certification de cybersécurité afin d'attester de la conformité des produits, services et processus aux exigences prévues par les schémas, selon une méthodologie d'évaluation précise, l'ANSSI a été désignée autorité nationale de certification de cybersécurité (ANCC) et doit à ce titre, au niveau national, superviser et faire respecter les règles prévues dans les schémas européens de certification de cybersécurité et contrôler le respect des obligations qui incombent aux fabricants ou fournisseurs de produits technologiques de l'information et de la communication. Ceci se traduit principalement par deux missions à assurer : la certification pour le niveau d'assurance élevé et la supervision de la mise en œuvre des schémas de certification de cybersécurité. Cette seconde mission inclut les activités de surveillance de marché pour les produits, services et processus autoévalués, de notification des organismes d'évaluation de la conformité et d'autorisation lorsque prévu par le schéma, de mise en œuvre d'un régime de sanctions

[178] Règlement (UE) n° 910/2014 du Parlement 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.

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

effectives, proportionnées et dissuasives, de mise en œuvre d'un système de gestion de réclamations, et de soutien à l'organisme national d'accréditation. La mise en œuvre du cadre laisse présager d'une multiplication du nombre de schémas de certification à opérer et d'éléments à certifier.

Enfin, depuis 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, l'autorité nationale de sécurité des systèmes d'information était chargée d'évaluer le niveau de sécurité des systèmes d'information d'importance vitale des opérateurs d'importance vitale ainsi que le respect des règles de sécurité fixées par arrêté du Premier ministre.

Une logique identique a conduit, lors de la transposition de la directive NIS, à soumettre au contrôle de l'autorité nationale de la sécurité des systèmes d'information les opérateurs de services essentiels et les fournisseurs de service numérique.

1.2. CADRE CONSTITUTIONNEL

L'article 34 de la Constitution prévoit que relèvent notamment du domaine de la loi les droits civiques et les garanties fondamentales accordées aux citoyens pour l'exercice des libertés publiques ; la liberté, le pluralisme et l'indépendance des médias ; les sujétions imposées par la défense nationale aux citoyens en leur personne et en leurs biens.

Le Conseil constitutionnel rattache la justification des prérogatives d'enquête et de contrôle des agents de l'Autorité des marchés financiers à la prévention des atteintes à l'ordre public et à la recherche des auteurs d'infractions (décision n° 2017-646/647 QPC du 20 juillet 2017, cons. 9). Certaines de ses décisions se réfèrent plus spécifiquement à un objectif de préservation de l'ordre public économique (décisions n° 2011-126 QPC du 13 mai 2011, n° 2012-280 QPC du 12 octobre 2012, n° 2021-892 QPC du 26 mars 2021).

A titre d'exemple, le Conseil constitutionnel considère que la définition des garanties appropriées et spécifiques relève de la loi lorsqu'une disposition peut affecter, par ses conséquences, le droit au respect de la vie privée et les garanties fondamentales accordées aux citoyens pour l'exercice des libertés publiques (décision n° 2004-499 DC du 29 juillet 2004).

Les missions de contrôle conférées à l'administration, pour lesquelles des pouvoirs d'investigation lui ont été confiés doivent tenir compte de principes constitutionnels tels que le respect du domicile, applicable également aux personnes morales, le droit à la vie privée et la protection des données à caractère personnel.

A ce titre, le Conseil d'Etat a rappelé dans un arrêt *Interconfort* du 6 novembre 2009 que : « Considérant qu'aux termes de l'article 8 de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales : 1. Toute personne a droit au respect de sa

vie privée et familiale, de son domicile et de sa correspondance. 2. Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui ; Considérant que si le droit au respect du domicile que ces stipulations protègent s'applique également, dans certaines circonstances, aux locaux professionnels où des personnes morales exercent leurs activités, il doit être concilié avec les finalités légitimes du contrôle, par les autorités publiques, du respect des règles qui s'imposent à ces personnes morales dans l'exercice de leurs activités professionnelles ; que le caractère proportionné de l'ingérence que constitue la mise en œuvre, par une autorité publique, de ses pouvoirs de visite et de contrôle des locaux professionnels résulte de l'existence de garanties effectives et appropriées, compte tenu, pour chaque procédure, de l'ampleur et de la finalité de ces pouvoirs ».

Ce faisant, lorsque des pouvoirs d'enquête et d'investigation sont confiés à l'administration menant à terme à une sanction, ils doivent être entourés de garanties suffisantes relatives notamment à l'impartialité, l'adéquation et la nécessité des mesures ainsi que le respect des droits de la défense et le contradictoire afin que les mesures de contrôle conservent un caractère proportionné.

Le Conseil constitutionnel admet que le niveau de garantie apporté aux pouvoirs d'enquête et d'investigation confiés à l'administration varie en fonction de l'organisme qui en est doté. En effet, dans une décision n° 2016-616/617 QPC du 9 mars 2017, il a considéré que : « Le principe de la séparation des pouvoirs, ni aucun autre principe ou règle de valeur constitutionnelle, ne font obstacle à ce qu'une autorité administrative non soumise au pouvoir hiérarchique du ministre, agissant dans le cadre de prérogatives de puissance publique, puisse exercer un pouvoir de sanction dans la mesure nécessaire à l'accomplissement de sa mission, dès lors que l'exercice de ce pouvoir est assorti par la loi de mesures destinées à assurer la protection des droits et libertés constitutionnellement garantis. En particulier, doivent être respectés le principe de la légalité des délits et des peines ainsi que les droits de la défense, principes applicables à toute sanction ayant le caractère d'une punition, même si le législateur a laissé le soin de la prononcer à une autorité de nature non juridictionnelle. Doivent également être respectés les principes d'indépendance et d'impartialité découlant de l'article 16 de la Déclaration de 1789 ».

La Cour européenne des droits de l'homme elle-même admet que « des impératifs de souplesse et d'efficacité, entièrement compatibles avec la protection des droits de l'homme, peuvent justifier l'intervention préalable d'organes administratifs […] ne satisfaisant pas sous tous leurs aspects [aux] prescriptions » de l'article 6§1 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales (CEDH, 23 juin 1981, *Le Compte, Van Leuven et De Meyere c/ Belgique,* n° 6878/75 et 7238/75, point 5).

Ainsi, est applicable aux sanctions administratives, notamment, le principe du respect des droits de la défense (Conseil d'Etat, Sect., 5 mai 1944, *Dame veuve Trompier-Gravier*, n° 69751 ; Conseil constitutionnel, n° 97-389 DC du 22 avril 1997, n° 99-411 DC du 16 juin 1999, n° 2001-451 DC du 27 novembre 2001). En ce qui concerne la motivation de la décision de sanction et le caractère contradictoire de la procédure, ce principe est formalisé dans le code des relations entre le public et l'administration (aux articles L. 211-1 et suivants, pour la motivation, et aux articles L. 121-1 et suivants, en particulier l'article L. 122-2, pour la procédure contradictoire). Ces garanties font l'objet des dispositions adaptées à ces principes dans le projet de loi.

S'agissant des sanctions administratives, si le Conseil constitutionnel a admis « qu'aucun principe ou règle de valeur constitutionnelle ne fait obstacle à ce qu'une autorité administrative, agissant dans le cadre de prérogatives de puissance publique, puisse exercer un pouvoir de sanction », il a ajouté que ce n'est qu'à la condition, « d'une part, que la sanction susceptible d'être infligée [soit] exclusive de toute privation de liberté et, d'autre part, que l'exercice du pouvoir de sanction [soit] assorti par la loi de mesures destinées à sauvegarder les droits et libertés constitutionnellement garantis » (Cons. const., n° 89-260 DC du 28 juillet 1989).

Bien que d'application plus souple pour certains, les sanctions administratives sont tenues au respect des principes de légalité des délits et des peines, de non rétroactivité des lois répressives plus sévères ou d'application immédiate des lois répressives plus douces, de nécessité et de proportionnalité des sanctions, d'individualisation des peines, de personnalité des peines ou encore d'égalité devant la loi.

1.3. CADRE CONVENTIONNEL

La Convention européenne des droits de l'homme, et en particulier son article 6 relatif au droit à un procès équitable est applicable dans le cadre de régimes de sanctions administratives, étant entendu que la Cour européenne des droits de l'homme admet une certaine souplesse dans la mise en œuvre des garanties : « des impératifs de souplesse et d'efficacité, entièrement compatibles avec la protection des droits de l'homme, peuvent justifier l'intervention préalable d'organes administratifs […] ne satisfaisant pas sous tous leurs aspects [aux] prescriptions » de l'article 6§1 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales (CEDH, 23 juin 1981, *Le Compte, Van Leuven et De Meyere c/ Belgique*, n° 6878/75 et 7238/75, point 5). Au demeurant, la mesure envisagée ne contrevient à aucune règle du droit conventionnel international.

1.4. ELEMENTS DE DROIT COMPARE

Le cadre du dispositif de contrôle et de sanctions découlant, pour l'essentiel, de règlements et de directives de l'Union européenne présente un niveau d'harmonisation élevé entre Etats membres de l'Union européenne, rendant une étude de droit comparé non pertinente.

2. NECESSITE DE LEGIFERER ET OBJECTIFS POURSUIVIS

2.1. NECESSITE DE LEGIFERER

Le règlement CSA dispose que les modalités de supervision susmentionnées s'appliquent à compter du 28 juin 2021. Le 31 janvier 2024, le premier schéma de certification européen, EUCC (EU *Common Criteria*), conforme aux réglementations européennes en matière de cybersécurité a été adopté avec des premiers certificats qui pourront être délivrés un an plus tard, soit à partir de début 2025. A cette date, il reviendra à l'ANCC de pouvoir jouer son rôle de supervision, ce qui nécessite que les pouvoirs d'enquête et de sanction de l'autorité nationale de sécurité des systèmes d'information soient définis dans la loi. Un régime de sanctions pour les violations au règlement lui-même doit être prévu mais aussi pour les violations des futurs schémas de certification européens attendus dans le cadre de règlements d'exécution.

Concernant le règlement eIDAS, il convient que l'autorité nationale de sécurité des systèmes d'information soit en mesure de sanctionner, le cas échéant, les acteurs qui ne respectent pas les exigences auxquelles ils sont soumis. Cela nécessite que les pouvoirs d'enquête et de sanction de l'autorité nationale de sécurité des systèmes d'information soient définis dans la loi.

S'agissant de la directive NIS 2, le délai de transposition fixé par le texte est le 17 octobre 2024. Le dispositif étant substantiellement modifié par rapport à la première directive, notamment à travers le périmètre des entités soumises au respect des obligations prévues par la directive, les pouvoirs de supervision et contrôles accordés à l'autorité nationale et l'introduction de sanctions administratives, une évolution des dispositions législatives en matière de pouvoirs d'enquête et de sanction de l'autorité nationale de sécurité des systèmes d'information est nécessaire.

Enfin, le dispositif de supervision instauré pour les besoins des textes précédents viendra modifier le régime de sanctions pénales prévu actuellement dans le dispositif SAIV pour son volet cyber, ce qui permettra une plus grande cohérence entre les régimes de sanctions applicables aux différentes réglementations.

La mise en œuvre de l'ensemble des réglementations susmentionnées nécessite ainsi de doter l'autorité nationale de sécurité des systèmes d'information des pouvoirs d'enquête et de police administrative suffisants pour assurer ses missions de contrôle, tout en rationalisant les dispositifs existants.

En effet, alors que les dispositifs existants conduisent à une saisine du juge pénal aux fins de prononcer une sanction, un régime de sanctions administratives vient s'ajouter pour assurer la mise en œuvre effective d'obligations portant sur les entités et autorités publiques concernées. Si l'autorité nationale est, jusqu'à présent, en charge de l'évaluation du niveau de sécurisation de systèmes d'information sensibles (article 1332-3 du code de la défense et articles 8 et 14 de la loi n° 2018-133), la transposition de la directive NIS 2 implique désormais de la doter de pouvoirs contraignants pour (i) rechercher et constater des manquements et (ii) prononcer des mesures d'exécution de se mettre en conformité, jusqu'à la notification des griefs en cas de respect par les entités concernées.

Bien qu'ils soient d'application immédiate, la mise en œuvre des règlements européens eIDAS et CSA implique également la définition des régimes de sanctions dans le droit national. L'article 16 du règlement eIDAS renvoie aux Etats membres le soin de fixer le régime des sanctions applicables là où l'article 65 du règlement CSA dispose que *« Les États membres déterminent le régime des sanctions applicables aux violations des dispositions du présent titre et aux violations des schémas européens de certification de cybersécurité et prennent toutes les mesures nécessaires pour assurer la mise en œuvre de ces sanctions »*.

De jurisprudence constante, il appartient à l'ordre juridique interne de chaque État membre, en vertu du principe de l'autonomie procédurale, de désigner les juridictions compétentes et de régler les modalités procédurales des recours destinés à assurer la sauvegarde des droits que les justiciables tirent du droit de l'Union (voir, en ce sens, arrêts du 30 septembre 2003, Köbler, C-224/01, EU:C:2003:513, point 47, et du 27 juin 2013, Agrokonsulting, C-93/12, EU:C:2013:432, point 35). Toutefois, la directive NIS 2 présente un degré de précision élevé quant aux pouvoirs et mesures d'exécution relevant de l'autorité compétente afin d'assurer la mise en œuvre effective de la directive.

Les principes de clarté et de simplification de la loi commandent de mutualiser les procédures de recherche et constatation des manquements en veillant à prévoir les garanties procédurales adéquates et protectrices des droits de la défense, dès lors que cette procédure aura vocation à conduire, le cas échéant à une sanction administrative.

Une loi est donc nécessaire pour doter l'autorité nationale de sécurité des systèmes d'information des pouvoirs et moyens requis dans le cadre d'une procédure d'instruction et de poursuite et de mettre à jour les dispositions législatives existantes.

Enfin, si les règlements eIDAS et CSA laissent le soin aux Etats membres de déterminer les sanctions applicables, la directive NIS 2 fixe elle-même les plafonds des sanctions, qu'il revient au droit national de reprendre *in extenso* sauf à encourir le risque de sous-transposer la directive.

Dans le même esprit de simplification que ci-dessus, les plafonds des sanctions ont été harmonisés avec ceux en cas de non-respect des règlements eIDAS et CSA, lesquels seront ainsi proportionnés et dissuasifs ainsi que ces textes le prescrivent.

2.2. OBJECTIFS POURSUIVIS

Le renforcement du rôle de l'autorité nationale, inscrit dans le présent projet de loi découle de plusieurs réglementations européennes en lien avec la sécurité numérique (en particulier, mais pas exclusivement, la transposition de la directive NIS 2) et nécessite la définition d'un cadre et de procédures pour garantir le bon fonctionnement, tant du point de vue de l'objectivité et de l'impartialité que de l'efficacité, des dispositifs de supervision prévus par ces réglementations, y compris l'instauration de procédures de contrôle et de mécanismes de sanction adaptés.

L'objectif est que ce cadre :

- fournisse la base juridique nécessaire à l'autorité nationale de sécurité des systèmes d'information pour mettre en œuvre le cadre juridique européen et assurer son rôle de supervision en lien avec les différentes réglementations européennes ;
- permette une mise en œuvre effective de sanctions graduées, proportionnées et dissuasives, dans des délais adaptés, créant de ce fait une réelle incitation au sein des entités concernées au respect de leurs obligations respectives et ainsi à adopter de bonnes pratiques en matière de cybersécurité ;
- tienne compte autant que possible d'une approche harmonisée entre les différents textes nationaux relatifs à la sécurité du numérique, ainsi qu'avec ceux liés à la résilience des entités critiques (directive REC[180]) ;
- présente des garanties suffisantes d'une procédure régulière, respectant les conditions d'un échange contradictoire ainsi que les principes généraux du droit, notamment en matière d'indépendance, d'impartialité et de respect des droits de la défense ;
- garantisse un haut niveau de cohérence entre les régimes de sanctions prévus par les différentes réglementations susmentionnées dans la mesure où certaines entités peuvent être soumises à plusieurs de ces réglementations.

3. OPTIONS ENVISAGEES ET DISPOSITIF RETENU

3.1. OPTIONS ENVISAGEES

[180] 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.

Mise à part pour quelques matières spécifiques précisées par décret, pour lesquelles certains ministères exerceront les compétences de l'autorité nationale de sécurité des systèmes d'information, les missions de supervision associées aux différentes réglementations en matière de cybersécurité susmentionnées sont confiées à l'ANSSI en tant qu'autorité nationale de sécurité des systèmes d'information.

Cette centralisation facilite le déploiement d'une approche coordonnée et cohérente des différentes facettes de la supervision en matière de cybersécurité. De par la possibilité pour l'ANSSI de déterminer, à partir de sa connaissance d'ensemble des enjeux de la cybersécurité, les priorités thématiques ou sectorielles pertinentes, cette approche pourra s'inscrire dans des programmes de contrôle qui pourraient être établis chaque année, dans le respect d'une logique de progressivité adaptée, liée à l'entrée en vigueur d'un nouveau cadre et à la nécessité pour les opérateurs de se l'approprier et de prendre les mesures adéquates pour satisfaire à l'ensemble de leurs nouvelles obligations. Cette position permettra ainsi d'assurer efficacement le pilotage du cadre réglementaire à venir, en proposant un socle de mesures et d'actions accessible, lisible, uniformisé et adapté aux différents niveaux de menace (cybercriminelle et étatique). C'est le choix qui a été fait dans les désignations des autorités nationales compétentes effectuées au titre des réglementations européennes précitées par note des autorités françaises auprès des autorités européennes, et qui est traduit dans la loi par les présentes dispositions.

Afin de rendre effectif le rôle de contrôle de l'autorité nationale de sécurité des systèmes d'information au service de ses missions de supervision, il est nécessaire d'habiliter ses agents à la recherche et à la constatation des manquements aux différentes réglementations susmentionnées, ainsi que de prévoir leur assermentation dans la mesure où ils seront amenés à effectuer des constats utilisés, le cas échéant, comme moyens de preuve venant étayer une décision de sanction. Ceux-ci doivent en outre être dotés de pouvoirs d'enquête suffisants pour l'accomplissement de cette mission, notamment les pouvoirs de réaliser des contrôles sur place ou sur pièces et de demander aux entités contrôlées toutes les informations et l'accès à leurs équipements nécessaires pour évaluer la conformité aux exigences et le respect des obligations leur incombant.

Le dispositif entend mettre à la charge des entités contrôlées le coût des mesures de contrôle prévues à l'article 29. Si la directive prévoit uniquement la prise en charge par les entités des audits ciblés lorsqu'ils sont réalisés par un organisme indépendant, un deuxième choix pouvait être de faire supporter aux entités les évaluations techniques et plus largement toute action de contrôle permettant de retenir l'application d'un principe de redevance pour service rendu, conformément à la jurisprudence du Conseil d'Etat[181], dans un souci d'harmonisation avec ce qui était d'ores et déjà prévu dans le cadre du dispositif SAIV (article L. 1332-6-3) et de la loi n° 2018-133 concernant les opérateurs de services essentiels.

[181] CE du 28 novembre 2028, n° 413839.

S’agissant de la nature et du niveau maximum des sanctions prévues en cas de manquement aux réglementations susmentionnées, ceux-ci doivent être fixés dans la loi. Là où la directive NIS 2 précise que ce sont des sanctions administratives qui doivent être prononcées, les règlements CSA et eIDAS ne spécifient pas leur nature. Dès lors, des sanctions administratives ou pénales pourraient être choisies. De même, la directive NIS 2 est prescriptive sur le niveau maximum des sanctions pécuniaires devant être fixé, tandis que les règlements CSA et eIDAS ne spécifient aucun montant. Concernant enfin le dispositif SAIV, il ne prévoit actuellement que des sanctions pénales. Sans contrevenir à ces textes, des natures de sanction et des montants soit identiques, soit différents, pourraient donc être prévus pour sanctionner les manquements à ces différentes réglementations.

Concernant la procédure de sanction, trois options sont envisageables :

Option 1 : attribuer à l’autorité nationale de sécurité des systèmes d’information la responsabilité d’instruire, de constater les manquements, de prendre les mesures de police administrative et de prononcer les sanctions administratives prévues dans la loi ;

Option 2 : charger l’autorité nationale de l’instruction, de la constatation des manquements et des mesures de police administrative, comme dans l’option 1, tandis qu’une commission des sanctions composée de magistrats et de personnalités compétentes, nommés indépendamment de l’autorité nationale est chargée de statuer sur les sanctions administratives prévues dans la loi ;

Option 3 : séparer entièrement de l’autorité nationale les missions liées au prononcé de sanctions, qui seraient exercées par une autorité différente, qu’elle soit administrative ou judiciaire.

3.2. DISPOSITIF RETENU

La recherche de cohérence dans la nature des sanctions dans le dispositif SAIV, tant pour son volet lié à la sécurité physique et à la résilience que pour son volet lié à la sécurité numérique, et dans la mise en œuvre de la directive NIS 2 et des règlements CSA et eIDAS, amène à retenir le principe de l’instauration de sanctions administratives applicables aux manquements de toutes ces réglementations. Adaptées au contexte de chaque réglementation, celles-ci prennent selon les cas la forme d’amendes administratives, d’une suspension de certaines activités pour une entité ou d’interdiction temporaire d’exercice de ses responsabilités par son dirigeant ou encore d’une abrogation d’une certification, d’une qualification ou d’une autorisation (article 37).

Le texte prévoit que le constat par l’autorité nationale de manquements aux obligations visées dans les chapitres II et III du projet de loi, qui instaure les régimes de sanctions prévus par les réglementations eIDAS, CSA, NIS 2 et SAIV (volet cyber), ne sera pas sanctionné

pénalement mais par une sanction administrative n'emportant donc pas inscription au casier judiciaire.

S'agissant du niveau maximum du montant des sanctions pouvant être prononcées dans la mise en œuvre des règlements CSA et eIDAS, par souci de cohérence du cadre de supervision de différentes réglementations qui ont en commun de concourir à une meilleure prise en compte des enjeux de cybersécurité et à une hausse du niveau de sécurité, il est préférable de ne pas multiplier les niveaux maximum de sanction étant entendu que la commission des sanctions aura la faculté de décider dans chaque cas d'un montant individualisé, proportionné à la gravité des faits dans la limite du niveau maximum à savoir 10 millions d'euros ou 2 % du chiffre d'affaires annuel mondial hors taxes ou 7 millions d'euros ou 1,4 % du chiffre d'affaires annuel mondial hors taxes en fonction des entités concernées.

Concernant la procédure de sanction, bien que le Conseil constitutionnel ait validé le principe selon lequel un service administratif peut prononcer des sanctions administratives[182], il est proposé d'écarter l'option 1, afin d'éviter tout risque de contentieux quant à l'impartialité des décisions. Concernant l'option 3, soit elle induirait des coûts administratifs disproportionnés du fait de la nécessité de doter l'autorité indépendante ainsi nouvellement créée de moyens matériels et de compétences techniques importants (cas de la création d'une autorité administrative indépendante), soit elle contribuerait à l'engorgement des services en charge de l'instruction des procédures judiciaires (cas du recours à une procédure pénale). Ces coûts n'apparaissent pas justifiés alors même que le dispositif de supervision prévu par NIS 2 permet de prendre toute une série de mesures contraignantes sans solliciter nécessairement l'intervention de l'autorité de sanction elle-même et que l'effet attendu du régime de sanction instauré devrait être principalement dissuasif et que, de ce fait, le nombre de sanctions prononcées devrait rester limité, au moins dans un premier temps.

Ainsi, il est proposé de retenir l'option 2, dans laquelle les rôles de supervision et d'instruction seront portés par l'autorité nationale tandis que la sanction administrative sera prononcée par une commission des sanctions indépendante, composée de magistrats du Conseil d'État, de la Cour de cassation et de la Cour des comptes, ainsi que de personnalités qualifiées. Il peut être relevé que cette option est en outre similaire à ce qui est mis en place pour de nombreuses autorités auxquelles est attribuée une compétence pour prononcer des sanctions administratives, dans la mesure où cela permet une séparation des fonctions d'instruction et de sanction[183], facteur offrant des garanties d'impartialité.

---

[182] Le conseil constitutionnel a en effet validé dans sa DC n° 2014-690 du 13 mars 2014 la possibilité pour un service administratif – en l'occurrence la DGCCRF – de relever des manquements à des dispositions relatives à la protection des consommateurs puis de prononcer des sanctions administratives (considérant 69).

[183] Voir par exemple l'AFA. C'est également similaire à ce qui est mis en place, suivant des modalités qui varient de l'une à l'autre, au sein des autorités administratives indépendantes (CNIL, AMF, ACPR, ARCEP, CRE, ARCOM, etc.).

Ainsi, à l'issue des contrôles réalisés par l'autorité nationale, dont la charge financière relève des entités contrôlées, et en cas de manquement constaté (articles 31 à 34), il pourra être adressé à l'opérateur une mise en demeure de se mettre en conformité, motivée et assortie d'un délai raisonnable émanant du directeur de l'autorité nationale, qui pourra en outre décider de la rendre publique (article 32). Les mesures d'exécution prises dans ce cadre pourront, le cas échéant, être accompagnées d'une astreinte au plus égale à 5 000 euros par jour de retard.

Si elle l'estime nécessaire, l'autorité nationale pourra, à l'issue du délai de mise en conformité précisé dans la mise en demeure et s'il est avéré que l'intéressé n'a pas apporté les preuves qu'il s'est mis en conformité, notifier à l'intéressé les griefs retenus et saisir la commission des sanctions. Cette dernière, après avoir entendu selon une procédure contradictoire l'intéressé, un représentant de l'autorité nationale et toute personne dont l'audition lui parait utile, statuera sur l'imposition d'une sanction et, le cas échéant, sur les modalités et, en cas de sanction pécuniaire, le quantum de cette sanction, qui doivent être proportionnés à la gravité des faits. Les sanctions prononcées par la commission des sanctions seront, le cas échéant, assorties d'une prise en charge financière par l'intéressé de la publication de la décision, s'il est décidé de la rendre publique.

Le continuum de mesures d'exécution et de sanctions pouvant être mises en œuvre, en cas de manquement constaté, par l'autorité nationale et, le cas échéant, la commission des sanctions si elle est saisie, offre ainsi une progressivité dans l'approche répressive.

4. ANALYSE DES IMPACTS DES DISPOSITIONS ENVISAGEES

4.1. IMPACTS JURIDIQUES

4.1.1. Impacts sur l'ordre juridique interne

Les articles 25 à 37 du présent projet de loi forment un chapitre III intitulé « De la supervision », au sein du Titre II.

4.1.2. Articulation avec le droit international et le droit de l'Union européenne

Les articles 8 (paragraphe 2), 32, 33, 34, 35 et 36 de la directive NIS 2 sont transposés dans les articles 25 à 37 du présent projet de loi, lesquels incluent également des dispositions d'adaptation du droit national aux règlements CSA (en particulier à ses articles 58 et 65) et eIDAS (en particulier à ses articles 16, 17).

4.2. IMPACTS ECONOMIQUES

4.2.1. Impacts macroéconomiques

Face à une menace toujours plus importante, des acteurs malveillants qui se professionnalisent et la multiplication des attaques, tous les secteurs et toutes les tailles d'entreprises et d'organisations sont touchés par les enjeux de la cybersécurité, avec un coût global important pour l'économie française.

Assurer un bon niveau de sécurité numérique général pour l'ensemble des entités avec des exigences particulières s'agissant des entités les plus sensibles, ce à quoi concourra l'exercice effectif des compétences de supervision, de contrôle et de sanction prévues par le présent projet de loi, sera par conséquent un facteur de renforcement de la compétitivité des entreprises françaises, de leur résilience et en conséquence de l'économie nationale.

Plus spécifiquement, en concourant à l'objectif principal de chacune de ces réglementations, le dispositif de supervision, de contrôle et de sanction proposé contribuera :

- au bon fonctionnement du marché européen numérique, qui est conditionné par la confiance que le grand public et les entreprises accordent aux produits, services et processus concernés, laquelle est renforcée par le recours à une certification de cybersécurité unifiée et mise en œuvre comme levier d'amélioration de leur sécurité (règlement CSA), ainsi que par la mise en œuvre d'un socle commun pour les interactions électroniques sécurisées entre les citoyens, les entreprises et les autorités publiques, qui accroit l'efficacité des services en ligne publics et privés et la sûreté des transactions électroniques (règlement eIDAS) ;
- à l'augmentation du niveau moyen de sécurité numérique des acteurs économiques, à la diminution de l'impact et donc du coût de la cybercriminalité en France, à l'augmentation de la demande sur le marché des solutions de sécurisation, à la diffusion large de la culture du risque cyber et à l'incitation des opérateurs à se conformer aux obligations réglementaires en la matière.

Le bon fonctionnement de la supervision qui peut faire intervenir diverses mesures à l'égard des entités assujetties (avertissement, injonctions, etc.) et, le cas échéant, des mécanismes de sanction est de nature à créer une incitation à la bonne application par un grand nombre d'entités des dispositions de différentes réglementations concourant, globalement, à la sécurité numérique. Il est en effet attendu de dispositifs efficaces de supervision et de contrôle et, le cas échéant, de sanction, conçus et mis en œuvre de manière objective, indépendante, proportionnée et réactive, un effet incitatif sur le plus grand nombre des entités assujetties.

4.2.2. Impacts sur les entreprises

Une partie des entités assujetties étant des entreprises, les impacts économiques identifiés ci-dessus s'appliquent également. Le bon fonctionnement de la supervision qui peut faire

intervenir diverses mesures à l'égard des entreprises assujetties et, le cas échéant, des mécanismes de sanction, est de nature à créer une incitation à la bonne application par un grand nombre d'entreprises des dispositions de différentes réglementations concourant, globalement, à la sécurité numérique et par conséquent à favoriser un environnement propice à la bonne conduite de leurs opérations et à l'accomplissement de leur rôle économique et social.

4.2.3. Impacts budgétaires

Le renforcement des dispositifs de supervision et de sanction (équipe dédiée en charge de la mise en œuvre de cette mission au sein de l'autorité nationale) ainsi que la création de la commission des sanctions généreront un coût de personnel et de fonctionnement pour l'Etat qui paraît mesuré, et en tout état de cause proportionné à l'objectif poursuivi.

4.3. IMPACTS SUR LES COLLECTIVITES TERRITORIALES

Une partie des entités assujetties étant des collectivités territoriales, les impacts micro-économiques identifiés ci-dessus peuvent être considérés s'appliquer à elles. Ainsi, le bon fonctionnement de la supervision est de nature à créer une incitation à la bonne application par un grand nombre de collectivités territoriales des dispositions de différentes réglementations concourant, globalement, à la sécurité numérique et, par conséquent, au bon accomplissement de leurs missions au service de leurs administrés.

4.4. IMPACTS SUR LES SERVICES ADMINISTRATIFS

L'application de sanctions administratives, à l'issue d'une procédure découlant d'une instruction par l'autorité nationale, permet d'éviter de contribuer à l'engorgement existant par ailleurs des services qui instruisent les procédures judiciaires, *a fortiori* avec des dossiers qui demandent souvent, de par leur technicité, une forte expertise en sécurité numérique pour en évaluer finement l'ensemble des enjeux.

La mesure proposée permet, pour autant, la séparation de la fonction décisionnelle en matière de sanctions des fonctions en charge des autres missions de l'autorité nationale (notamment : sensibilisation, assistance technique, formation, mise en œuvre de dispositifs de détection, recueil d'informations techniques relatives aux incidents affectant les systèmes d'information et concours à la réponse à ces incidents,), ainsi que de la fonction responsable du pilotage des missions de contrôle et de l'instruction des dossiers, tout en maintenant cette dernière au sein des services de l'autorité nationale, lui permettant de bénéficier du haut niveau de technicité et de connaissance du secteur de la cybersécurité développés au sein de l'autorité nationale, ce que l'option 3 *supra* n'aurait pas permis. Des mesures organisationnelles internes à l'autorité nationale permettront en outre à celle-ci de s'assurer qu'en son sein des modalités de

fonctionnement pertinentes soient trouvées entre la fonction responsable du pilotage des missions de contrôle et de l'instruction des dossiers, d'une part, et les fonctions assurant des missions de conseil aux opérateurs (notamment : sensibilisation, assistance technique, formation, mise en œuvre de dispositifs de détection, recueil d'informations techniques relatives aux incidents affectant les systèmes d'information et concours à la réponse à ces incidents) d'autre part, pour préserver la confiance placée par les opérateurs dans les échanges qu'ils ont avec l'administration dans les différents contextes que ceux-ci peuvent prendre.

Par ailleurs, l'autorité nationale est déjà identifiée par les entités dans son rôle d'accompagnement pour leur permettre d'élever le niveau de sécurité de leurs systèmes d'information, rôle qui devra, dans le fonctionnement de l'autorité nationale, être élargi et renforcé pour tenir compte de la diversité des secteurs concernés et du nombre des entités assujetties à la directive NIS 2.

4.5. IMPACTS SOCIAUX (EMPLOI / HANDICAP, EGALITE HOMMES-FEMMES)

4.5.1. Impacts sur la société

Les mesures proposées peuvent avoir un effet indirect sur l'emploi, au travers d'un besoin croissant de personnel dans les fonctions liées à la cybersécurité dans les organisations ainsi que chez les fournisseurs de solutions de cybersécurité (produits et services), tandis qu'en encourageant le renforcement du niveau de sécurité d'opérateurs économiques elle permet également de contribuer à leur solidité financière, et donc à préserver des emplois qui seraient menacés en cas d'attaque à fort impact sur une ou plusieurs entités.

4.5.2. Impacts sur les personnes en situation de handicap

Sans objet.

4.5.3. Impacts sur l'égalité entre les femmes et les hommes

Sans objet.

4.5.4. Impacts sur la jeunesse

Sans objet.

4.5.5. Impacts sur les professions réglementées

Sans objet.

4.6. IMPACTS SUR LES PARTICULIERS

L'encouragement au renforcement du niveau de sécurité numérique des entités assujetties à la directive NIS2 induit par les mesures de contrôle et de sanction est de nature à favoriser un environnement de confiance pour les particuliers, en tant que clients des entreprises et administrés des administrations.

4.7. IMPACTS ENVIRONNEMENTAUX

Le fonctionnement des équipes de l'autorité nationale en charge de l'activité de supervision et de contrôle ainsi que de la commission des sanctions générera une activité additionnelle de nature administrative, qui sera homogène aux activités déjà existantes de l'autorité nationale.

Les impacts attendus en matière environnementale (induits par la consommation d'énergie, de produits consommables, les déplacements, etc.) paraissent dès lors non spécifiques à cette activité et, en tout état de cause, mesurés au vu de l'objectif poursuivi.

5. CONSULTATIONS ET MODALITES D'APPLICATION

5.1. CONSULTATIONS MENEES

Conformément aux dispositions de l'article L. 1212-2 du code général des collectivités territoriales, la présente disposition a été soumise à l'examen du Conseil national d'évaluation des normes (CNEN) qui a rendu un avis défavorable le 22 mai 2024.

La Commission supérieure du numérique et des postes (CSNP) a été consultée sur les présentes dispositions. Elle a rendu un avis n° 2024-03 le 21 mai 2024 appelant à s'assurer de la clarté du périmètre des entités concernées et des mesures qu'elles devront appliquer ainsi qu'à mettre en œuvre une stratégie d'accompagnement à la mise en conformité et une politique de supervision progressive.

Sur le fondement de l'article 8 de la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, la Commission nationale de l'informatique et des libertés (CNIL) a été consultée à titre facultatif. Elle a rendu un avis favorable le 23 mai 2024 au renforcement des mesures en matière de cybersécurité, appelant toutefois à s'assurer de la cohérence des exigences de sécurité découlant des principes relatifs à la protection des données avec celles issues de la directive NIS 2 ainsi qu'à une coordination entre la CNIL et l'ANSSI sur la mise en œuvre de NIS 2.

Un travail a été mené depuis plusieurs années pour bâtir un écosystème relais de confiance : CSIRT ministériels, sectoriels ou territoriaux ou prestataires qualifiés, avec lesquels l'ANSSI échange régulièrement.

5.2. MODALITES D'APPLICATION

5.2.1. Application dans le temps

Les présentes dispositions entrent en vigueur le lendemain de la publication de la présente loi au *Journal officiel* de la République française.

5.2.2. Application dans l'espace

Les dispositions s'appliqueront sur l'ensemble du territoire national.

S'agissant des sanctions pécuniaires (articles 28 et 37), elles seront prononcées en monnaie locale pour ce qui concerne les entités établies dans les îles Wallis et Futuna, en Polynésie française et en Nouvelle-Calédonie.

5.2.3. Texte d'application

L'article 30 prévoit que des mesures de caractère réglementaire à prendre par voie de décret en Conseil d'État préciseront les modalités d'application des dispositions de la Section 1, notamment relativement à la recherche et aux constations des manquements.

L'article 34 prévoit qu'un décret en Conseil d'Etat fixe les modalités de la procédure d'instruction.

Par ailleurs, comme mentionné *supra*, les conditions de fonctionnement de la commission des sanctions seront également définies par décret en Conseil d'Etat, prévu à l'article L. 1332-14 du code de la défense.

CHAPITRE IV – DISPOSITIONS DIVERSES D'ADAPTATION

Article 38 – Alléger le contrôle des biens de cryptologie

1. ÉTAT DES LIEUX

1.1. CADRE GENERAL

On entend par moyen de cryptologie tout matériel ou logiciel conçu ou modifié pour transformer des données, qu'il s'agisse d'informations ou de signaux, à l'aide de conventions secrètes ou pour réaliser l'opération inverse avec ou sans convention secrète.

Le régime de contrôle des moyens et prestations de cryptologie relève actuellement de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN) et son décret d'application n° 2007-663 du 2 mai 2007 modifié.

L'article 30 de la loi prévoit une utilisation libre des moyens de cryptologie, quelle que soit leur fonction. Il prévoit également la fourniture, le transfert depuis un Etat membre, l'export et l'import libres de moyens de cryptologie ayant des fonctions d'authentification et d'intégrité.

Toutefois, il impose un régime de déclaration préalable auprès du Premier ministre pour la fourniture, l'import et les transferts depuis et vers un Etat membre de moyens de cryptologie n'assurant pas exclusivement des fonctions d'authentification ou de contrôle d'intégrité. Le même régime déclaratif est prévu pour la fourniture de prestations de cryptologie du même type en vertu de l'article 31 de la même loi.

Enfin, l'article 30 impose un régime d'autorisation préalable pour l'export vers un Etat membre de l'Union européenne de ces mêmes moyens. Aux termes du décret n°2007-663 précité, les autorisations d'exportation sont délivrées pour une durée qui ne peut excéder cinq ans et doivent être renouvelées passé ce délai.

Le décret n° 2007-663 précise les modalités d'application des articles 30 et 31, et dispose notamment que c'est à l'ANSSI que les déclarations et demandes d'autorisation d'exportation sont adressées.

Cette réglementation coexiste avec celle relative aux biens à double usage (BDU), à savoir les biens, produits ou technologies essentiellement civils, sujets au risque de détournement d'usage à des fins militaires prohibées ou de prolifération nucléaire, biologique ou chimique, dont l'exportation est contrôlée, à laquelle certains moyens de cryptologie sont également soumis. Aussi, lorsqu'un BDU intègre un dispositif de cryptologie, il faut une autorisation

préalable d'exportation de bien de cryptologie délivrée par l'ANSSI, puis une autorisation de licence d'exportation de BDU relevant du régime général. La réglementation européenne[184] est notamment précisée par le décret n° 2001-1192 du 13 décembre 2001 relatif au contrôle à l'exportation, à l'importation et au transfert des biens et technologies à double usage (modifié pour tenir compte du règlement européen de 2009) et par l'arrêté du 13 décembre 2001 relatif au contrôle à l'exportation vers les pays tiers et au transfert vers les Etats membres de la Communauté européenne de biens et technologies à double usage.

Ce dernier texte précise que l'autorisation d'exportation est un préalable à une demande de licence pour les moyens de cryptologie[185]. Ce contrôle, en deux étapes ayant chacune leurs délais propres, est donc perçu comme un double contrôle pénalisant pour l'export depuis la France.

A ses articles 32 et 33, la loi n° 2004-575 du 21 juin 2004 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.

1.2. CADRE CONSTITUTIONNEL

L'objectif de valeur constitutionnelle d'intelligibilité de la loi assure la lisibilité des textes et prohibe la complexité inutile[186].

1.3. CADRE CONVENTIONNEL

L'objet de l'article est lié au règlement (UE) 2021/821 du Parlement européen et du Conseil du 20 mai 2021 instituant un régime de l'Union de contrôle des exportations, du courtage, de l'assistance technique, du transit et des transferts en ce qui concerne les biens à double usage.

2. NECESSITE DE LEGIFERER ET OBJECTIFS POURSUIVIS

[184] Règlement (UE) n° 2021/821 du Parlement européen et du Conseil du 20 mai 2021 instituant un régime de l'Union de contrôle des exportations, du courtage, de l'assistance technique, du transit et des transferts en ce qui concerne les biens à double usage (refonte) reprenant elle-même, dans son annexe modifiée chaque année, les textes de l'*Arrangement de Wassenaar* sur le contrôle des exportations d'armes conventionnelles et de biens et technologies à double usage.

[185] Sauf exception pour lesquelles une déclaration est suffisante.

[186] Cons. const., n° 2003-473 DC, 26 juin 2003, cons. 5.

2.1. NECESSITE DE LEGIFERER

Le régime de contrôle des moyens et prestations de cryptologie relève actuellement de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN). Sa modification implique une disposition de niveau législatif.

2.2. OBJECTIFS POURSUIVIS

L'objectif est d'alléger la charge pour les entreprises et l'administration.

Le régime d'autorisation préalable à l'exportation de moyens de cryptologie prévu par la loi n° 2004-575 susmentionnée poursuit le même objectif que le régime d'autorisation préalable à l'exportation des biens à double usages prévu par le règlement 2021/821. Ce doublon réglementaire est source d'incompréhension pour les entreprises exportatrices qui ne comprennent pas pourquoi, en France, l'administration exige deux autorisations différentes pour la même opération d'exportation. Cette double procédure rallonge nécessairement le délai des formalités administratives en amont de la commercialisation des produits, ce qui nuit à la réactivité des entreprises françaises et peut, dans certains cas, obérer leur compétitivité face à des acteurs étrangers, y compris européens.

Pour l'administration, le traitement des demandes d'autorisation d'exportation prévues par la loi n° 2004-575 précitée, en plus des demandes d'autorisation d'exportation de BDU, est une charge dont elle pourrait utilement faire l'économie. Cette charge est d'autant plus conséquente que l'utilisation de moyens de cryptologie s'est largement démocratisée : des fonctions de cryptographie sont désormais embarquées dans de très nombreux produits. Aujourd'hui, ce seul dispositif nécessite trois ETP, lesquels traitent en moyenne cinq cent demandes par an.

En tout état de cause, au cours des cinq dernières années aucun refus n'a été délivré en réponse à une demande d'autorisation d'exportation déposée en application de la loi n° 2004-575 précitée, ce qui tend à montrer que, dans les faits, ce dispositif n'a pas de véritable utilité.

3. OPTIONS ENVISAGEES ET DISPOSITIF RETENU

3.1. OPTIONS ENVISAGEES

Outre le dispositif retenu, deux options étaient envisageables :

- le maintien des régimes actuels de déclaration et demande d'autorisation d'exportation, ce qui laisse persister des contraintes fortes allant à l'encontre du principe de simplification du droit ;

- la suppression des deux régimes de déclaration et d'autorisation d'exportation, ce qui permet un allégement total de la charge administrative. Toutefois, elle fait disparaitre intégralement ce mécanisme de recueil d'informations techniques sur les moyens de cryptologie circulant en France et pose donc des difficultés en termes de sécurité car elle réduit la connaissance qu'a l'administration des moyens utilisés pour garantir la confidentialité des échanges d'information.

3.2. DISPOSITIF RETENU

Le projet de loi retient la transformation du régime d'autorisation en régime déclaratif. Cette option offre un bon équilibre entre, d'une part, l'objectif de simplification du droit et, d'autre part, la nécessité de maintenir une veille technique sur les moyens de cryptologie circulant en France. En effet, cette mesure apporte un allègement de la charge sur l'exportation. Même si elle ne simplifie pas les démarches imposées pour l'importation et la fourniture en France de moyens de cryptologie, elle permet néanmoins, grâce au régime unique de déclaration applicable à toutes les opérations, d'alléger la charge pour l'administration et de maintenir un dispositif de contrôle et de recueil d'informations techniques sur les moyens de cryptologie circulant en France.

En cohérence avec la suppression du régime d'autorisation, le I de l'article 35 de la loi n° 2004-575 est modifié pour supprimer les sanctions prévues en cas de défaut d'obtention d'autorisation.

L'article 33 de la loi n° 2004-575 précitée prévoit un régime de responsabilité des prestataires de services de certification électronique. Les principes énoncés dans cet article sont rendus obsolètes et en partie incohérents avec les dispositions prévues à l'article 13 du règlement 910/2014 dit « eIDAS ». En effet, l'article 33 de la loi n° 2004-575 prévoit que « *Sauf à démontrer qu'ils n'ont commis aucune faute intentionnelle ou négligence, les prestataires de services de certification électronique sont responsables du préjudice causé aux personnes qui se sont fiées raisonnablement aux certificats présentés par eux comme* ***qualifiés*** […] ». Le règlement eIDAS, quant à lui, prévoit à son article 13 un régime général de responsabilité du prestataire de service de confiance, que ce dernier soit qualifié ou non : « *Sans préjudice du paragraphe 2, les prestataires de services de confiance sont responsables des dommages causés intentionnellement ou par négligence à toute personne physique ou morale en raison d'un manquement aux obligations prévues par le [règlement eIDAS]* ».

4. ANALYSE DES IMPACTS DES DISPOSITIONS ENVISAGEES

4.1. IMPACTS JURIDIQUES

4.1.1. Impacts sur l'ordre juridique interne

Cette mesure modifie les articles 30 et 35 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN). Elle abroge l'article 33 de la même loi. Elle impacte également l'article 57 de la loi du 21 juin 2004 relative aux dispositions ultra-marines en raison des renvois (voir l'article 40 du présent projet de loi).

4.1.2. Articulation avec le droit international et le droit de l'Union européenne

Les dispositions envisagées s'articulent avec le règlement 2021/821 du 20 mai 2021. Ce règlement prévoit en effet les modalités de contrôle à l'export des moyens de cryptologie ainsi que le périmètre de contrôle à savoir les biens listés à l'annexe I, catégorie 5, partie 2.

Ce règlement prévoit également les modalités de contrôle pour les transferts vers un autre Etat membre des biens de la catégorie 5, partie 2 listés à l'annexe IV. Le paragraphe 8 de l'article 11 prévoit par ailleurs qu'un État membre peut, par sa législation nationale, exiger que, pour tout transfert intra-Union au départ de cet État membre de biens visés à l'annexe I, catégorie 5, partie 2, qui ne sont pas énumérés à l'annexe IV, des informations complémentaires concernant ces biens soient fournies à ses autorités compétentes.

Le décret en Conseil d'Etat devra assurer la cohérence avec ce règlement en particulier pour la définition des catégories de moyens dispensés de formalités préalables pour l'exportation ou le transfert vers un autre Etat membre.

4.2. IMPACTS ECONOMIQUES ET FINANCIERS

4.2.1. Impacts macroéconomiques

Sans objet.

4.2.2. Impacts sur les entreprises

Cette modification supprimera pour les exportateurs une formalité administrative, ce qui améliorera la lisibilité de la procédure dont ils doivent s'acquitter en amont d'une exportation et contribuera à leur réactivité commerciale. Plus généralement, elle impliquera un allègement pour les exportateurs de moyens de cryptologie en termes de délai avant exportation.

4.2.3. Impacts budgétaires

Sans objet.

4.3. IMPACTS SUR LES COLLECTIVITES TERRITORIALES

Sans objet.

4.4. IMPACTS SUR LES SERVICES ADMINISTRATIFS

Cf. § « Objectifs poursuivis ».

4.5. IMPACTS SOCIAUX

4.5.1. Impacts sur la société

Sans objet.

4.5.2. Impacts sur les personnes en situation de handicap

Sans objet.

4.5.3. Impacts sur l'égalité entre les femmes et les hommes

Sans objet.

4.5.4. Impacts sur la jeunesse

Sans objet.

4.5.5. Impacts sur les professions réglementées

Sans objet

4.6. IMPACTS SUR LES PARTICULIERS

Sans objet.

4.7. IMPACTS ENVIRONNEMENTAUX

Sans objet.

5. CONSULTATIONS ET MODALITES D'APPLICATION

5.1. CONSULTATIONS MENEES

Ces dispositions n'ont pas fait l'objet de consultation spécifique des acteurs industriels, qui ont déjà, à de nombreuses occasions, fait connaître leur opposition au double régime de contrôle actuel, et leur souhait de voir les contraintes allégées au maximum.

Conformément aux dispositions de l'article L. 1212-2 du code général des collectivités territoriales, la présente disposition a été soumise à l'examen du Conseil national d'évaluation des normes (CNEN) qui a rendu un avis défavorable le 22 mai 2024.

Enfin, sur le fondement de l'article 8 de la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, la Commission nationale de l'informatique et des libertés (CNIL) a été consultée à titre facultatif.

5.2. MODALITES D'APPLICATION

5.2.1. Application dans le temps

Ces dispositions entrent en vigueur au lendemain de la publication de la loi au *Journal officiel* de la République française.

5.2.2. Application dans l'espace

Conformément à l'article 40 du présent projet de loi, le titre II est applicable dans les îles Wallis et Futuna, en Polynésie française, en Nouvelle-Calédonie et dans les Terres australes et antarctiques françaises, sous réserve des adaptations suivantes :

1° 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, applicables localement.

2° Dans les îles Wallis et Futuna, en Polynésie française et en Nouvelle-Calédonie, les sanctions pécuniaires encourues en vertu du titre II de la présente loi sont prononcées en monnaie locale, compte tenu de la contre-valeur de l'euro dans cette monnaie.

Pour l'application du titre II à Saint-Barthélemy, Saint-Pierre-et-Miquelon, dans les îles Wallis et Futuna, en Polynésie française, en Nouvelle-Calédonie et dans les Terres australes et antarctiques françaises, les références à la directive (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 et aux règlements de l'Union

européenne sont remplacées par la référence aux règles en vigueur en métropole en vertu de la même directive et des mêmes règlements.

Enfin, conformément à l'article 40 du présent projet de loi, l'article 57 de la loi du 21 juin 2004 est modifié pour l'application de cette loi en Nouvelle-Calédonie, en Polynésie française, à Wallis-et-Futuna, dans les Terres australes et antarctiques françaises et à Mayotte

5.2.3. Textes d'application

Les décrets suivants devront être modifiés :

- Décret en Conseil d'Etat n° 2007-663 du 2 mai 2007 pris pour l'application des articles 30, 31 et 36 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique et relatif aux moyens et aux prestations de cryptologie ;
- 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 » ;
- Arrêté du 13 décembre 2001 relatif au contrôle à l'exportation vers les pays tiers et au transfert vers les Etats membres de la Communauté européenne de biens et technologies à double usage.

En outre, l'arrêté du 29 janvier 2015 définissant la forme et le contenu des dossiers de déclaration et de demande d'autorisation d'opérations relatives aux moyens et aux prestations de cryptologie devra être modifié.

Article 39 (I, II et III) - Abrogation de la transposition de la directive NIS 1 et simplification du cadre réglementaire

1. ÉTAT DES LIEUX

1.1. CADRE GENERAL

1.1.1. Ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives

L'ordonnance n° 2005-1516 du 8 décembre 2005 introduit le référentiel général de sécurité (RGS) qui impose aux autorités administratives[187] la mise en œuvre de mesures de sécurité visant à limiter la fraude liée à l'usage des services numériques de ces administrations pour échanger avec leurs usagers ou d'autres administrations (par exemple : l'identification électronique, la signature / le cachet électronique, l'horodatage électronique). L'ordonnance n° 2005-1516 du 8 décembre 2005 s'accompagne du décret 2010-112 du 2 février 2010 et de l'arrêté du 13 juin 2014 portant approbation de la dernière version RGS.

Périmètre organique

Trois types d'acteurs sont concernés par le RGS :

- L'autorité administrative qui se voit imposer des obligations dans ces échanges par voie électronique avec ses usagers ou d'autres autorités administratives,
- Les prestataires de services de confiance ou des fournisseurs qui peuvent, sur la base du volontariat, qualifier leurs produits de sécurité ou leurs services de confiance en vue de les proposer aux autorités administratives pour faciliter leur mise en conformité aux obligations,
- Les organismes délivrant des décisions de qualification des prestataires de services de confiance.

[187] Les administrations de l'État, les collectivités territoriales, les établissements publics à caractère administratif, les organismes gérant des régimes de protection sociale relevant du code de la sécurité sociale et du code rural ou mentionnés aux articles L. 223-16 et L. 351-21 du code du travail et les autres organismes chargés de la gestion d'un service public administratif ainsi que les commissions de coordination des actions de prévention des expulsions locatives prévues à l'article 7-2 de la loi n° 90-449 du 31 mai 1990 visant à la mise en œuvre du droit au logement.

Périmètre technique

Le RGS s'applique aux seuls systèmes d'information mis en œuvre par les autorités administratives et qui supportent des échanges par voie électronique entre ces autorités administratives et leurs usagers ou entre autorités administratives elles-mêmes (par exemple : impots.gouv.fr, le site internet d'une collectivité territoriale permettant à un administré de payer les frais de cantine, le site internet du Conseil d'État).

Mesures de sécurité

Le RGS prévoit des mesures liées à la protection des échanges par voie électronique entre l'autorité administrative mettant en œuvre le système qui supporte ces échanges et les usagers ou d'autres autorités administratives.

Lorsqu'une autorité administrative recourt à des produits de sécurité ou à des prestataires de services de confiance ayant fait l'objet d'une qualification, cette administration peut se prévaloir d'une présomption de conformité aux exigences du RGS.

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

Les articles 1 à 15 de la loi n° 2018-133 du 26 février 2018 transposent en droit national les dispositions de la directive n° 2016/1148 du 6 juillet 2016 dite NIS 1, dont l'objectif majeur est d'assurer un niveau de sécurité élevé et commun pour les réseaux et les systèmes d'information de l'Union européenne.

Cette loi s'accompagne du décret n° 2018-384 du 23 mai 2018 qui précise les dispositions relatives à la sécurité des réseaux et des systèmes d'information des OSE et des fournisseurs de services numériques et de plusieurs arrêtés[188] du Premier ministre précisant notamment les modalités de déclaration des incidents de sécurité ainsi que les règles de sécurité devant être mises en œuvre.

[188] Arrêté du 13 juin 2018 fixant les modalités des déclarations prévues aux articles 8, 11 et 20 du décret n° 2018-384 du 23 mai 2018 relatif à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels et des fournisseurs de service numérique - Légifrance (legifrance.gouv.fr)

Arrêté du 14 septembre 2018 fixant les règles de sécurité et les délais mentionnés à l'article 10 du décret n° 2018-384 du 23 mai 2018 relatif à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels et des fournisseurs de service numérique - Légifrance (legifrance.gouv.fr)

Arrêté du 1er août 2018 relatif au coût d'un contrôle effectué par l'Agence nationale de la sécurité des systèmes d'information en application des articles 8 et 14 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 - Légifrance (legifrance.gouv.fr)

Périmètre organique

Prenant pour modèle le volet cyber du dispositif national de sécurité des activités d'importance vitale (SAIV) prévu par le code de la défense, cette loi prévoit la désignation d'opérateurs de services essentiels (OSE). Ces OSE sont désignés par le Premier ministre au regard de leurs activités, qui s'inscrivent dans un secteur défini dans la transposition nationale et reprenant au minimum ceux listés dans la directive NIS 1.

Cette loi vise également les fournisseurs de services numériques qui couvre les services d'informatique en nuage (opérateurs de cloud), les places de marché en ligne, les moteurs de recherche.

Périmètre technique

Ces OSE sont tenus de déclarer à l'ANSSI leurs systèmes d'information essentiels (SIE) répondant à des critères définis au niveau réglementaire et sur lesquels ces opérateurs devront appliquer des mesures de sécurité.

Mesures de sécurité

Les mesures de sécurité définies dans le cadre de NIS 1 reprennent celles définies dans le cadre du volet cyber du dispositif SAIV et dont les exigences ont été allégées pour tenir compte des enjeux visés par la directive et de la maturité des OSE.

1.1.3. Modification de certaines dispositions du code de la défense

Les opérateurs mentionnés aux articles L. 1332-1 et L. 1332-2 du code de la défense (appelés « opérateurs d'importance vitale » ou « OIV ») doivent mettre en œuvre des règles de sécurité nécessaires à la protection de leurs systèmes d'information pour lesquels l'atteinte à la sécurité ou au fonctionnement risquerait de diminuer d'une façon importante le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la Nation ou pourrait présenter un danger grave pour la population, obligation étendue aux systèmes d'information des opérateurs publics ou privés qui participent à ces systèmes (article L. 1332-6-1 du code de la défense).

1.2. CADRE CONSTITUTIONNEL

Principe de libre administration des collectivités territoriales

La directive s'applique aux administrations centrales et régionales. Par ailleurs, elle laisse la possibilité aux Etats membres d'en appliquer les dispositions aux administrations locales.

Le projet de loi impose des obligations aux régions, aux départements, aux grandes communes et à certains groupements, mais également à certains établissements publics locaux.

Le principe de libre administration des collectivités territoriales figure à l'article 72 de la Constitution de 1958. Repris dans le code général des collectivités territoriales, la libre administration est un principe à valeur constitutionnelle [189] qui s'impose au législateur et à toutes les autorités administratives. Le fait d'imposer des obligations aux collectivités territoriales touche au principe de leur libre administration et nécessite de légiférer[190].

Régime des obligations civiles et commerciales

L'article 34 de la Constitution prévoit notamment que la loi détermine les principes fondamentaux des obligations civiles et commerciales. Ainsi, une loi qui impose des obligations à des entreprises privées doit déterminer précisément le périmètre des entreprises soumises à ces obligations[191] .

Le projet de loi détermine avec précision les critères qui permettent de définir les entités essentielles et les entités importantes soumises aux mesures de gestion des risques de cybersécurité sur leurs systèmes d'information et réseaux.

Intelligibilité de la loi

La simplification et la rationalisation du cadre législatif et règlementaire est nécessaire compte tenu de l'enchevêtrement des notions et des champs d'application entre d'une part, la directive NIS 2, et d'autre part, les législations internes existantes. En effet, l'objectif de valeur constitutionnelle d'intelligibilité de la loi assure la lisibilité des textes, prohibe la complexité inutile (Cons. const., n° 2003-473 DC, 26 juin 2003, cons. 5.) et excessive de la loi au regard de l'aptitude de ses destinataires (Cons. const., n° 2005-530 DC, 29 déc. 2005, cons. 77.), favorise la simplification du texte législatif (Cons. const., n° 2003-473 DC, 26 juin 2003, cons. 5 ; n° 2004-506 DC, 2 déc. 2004, cons. 5.), soutient la codification, notamment à droit constant (Cons. const., n° 2003-473 DC, 26 juin 2003, cons. 5 ; n° 99-421 DC, 16 déc. 1999, cons. 13 ; n° 2004-506 DC, 2 déc. 2004, cons. 5), combat la contradiction et l'inintelligibilité (Cons. const., n° 2001-447 DC, 18 juill. 2001, cons. 27.), et pose une exigence de précision (Cons. const., n° 2000-437 DC, 19 déc. 2000, cons. 3.).

1.3. CADRE CONVENTIONNEL

[189] Cons. const. 23 mai 1979, n° 79-104 DC, § 9.

[190] Cons. const. 10 mars 1988, n° 88-154 L, § 4.

[191] Cons. const. 13 août 2015, n° 2015-718 DC

L'article 44 de la directive 2022/2555 dite NIS 2 vient abroger les dispositions de la directive (UE) 2016/1148 dite NIS1. L'article 39 du projet de loi prévoit notamment l'abrogation des dispositions de la loi n° 2018-133 transposant la directive NIS1.

2. NECESSITE DE LEGIFERER ET OBJECTIFS POURSUIVIS

2.1. NECESSITE DE LEGIFERER

Etant donné que le projet de loi porte la transposition de la directive NIS2 abrogeant elle-même la directive NIS1, le projet de loi prévoit au II. de l'article 39 l'abrogation des dispositions de la loi n° 2018-133 transposant la directive NIS1 et au III du même article les dispositions du code de la défense faisant référence à cette loi.

Le projet de loi embarque également des dispositions relatives à la simplification du cadre réglementaire cyber et en particulier le référentiel général de sécurité (RGS) porté par l'ordonnance de 2005.

2.2. OBJECTIFS POURSUIVIS

2.2.1. Ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives

Périmètre organique

L'ordonnance n° 2005-1516 définit, dans son article 1, la notion d'autorité administrative couvrant « les administrations de l'État, les collectivités territoriales, les établissements publics à caractère administratif, les organismes gérant des régimes de protection sociale relevant du code de la sécurité sociale et du code rural ou mentionnés aux articles L. 223-16 et L. 351-21 du code du travail et les autres organismes chargés de la gestion d'un service public administratif ».

Dans un souci de simplification et d'harmonisation des exigences applicables, seules les administrations qui seront assujetties à la transposition nationale de la directive NIS 2 seront par ailleurs assujetties au RGS.

Périmètre technique

Le RGS conservera le périmètre technique actuel, à savoir les systèmes d'information que les administrations mettent en œuvre et qui supportent des échanges par voie électronique entre ces administrations et leurs usagers ou entre administrations elles-mêmes (*par exemple :*

impots.gouv.fr, le site internet d'une collectivité territoriale permettant à un administré de payer les frais de cantine, le site internet du Conseil d'État).

Mesures applicables

Il est prévu des mesures spécifiques, complémentaires au socle commun de cybersécurité qui s'appliquera aux administrations assujetties à la transposition nationale de la directive NIS 2. Ces mesures auront pour finalité de limiter la fraude liée à l'usage des services numériques de l'administration (par exemple dans le champ de l'identification électronique, la signature / le cachet électronique, l'horodatage électronique). Il est prévu également un mécanisme de présomption de conformité aux exigences du RGS pour les administrations qui recourent à des prestataires de services de confiance détenant une décision de qualification.

Abrogation des dispositions de l'ordonnance

Les dispositions de l'article 9 de l'ordonnance n° 2005-1516 définissant les obligations pour les autorités administratives sont abrogées car désormais portées par les dispositions du troisième alinéa de l'article 15 du projet de loi.

Les dispositions de l'article 12 de l'ordonnance n° 2005-1516 relatives au référencement des produits de sécurité et prestataires de services de confiance qualifiés sont abrogées car abandonnées.

Les dispositions du I. de l'article 14 de l'ordonnance n° 2005-1516 relatives au délai de mise en conformité au RGS sont abrogées.

Les définitions des notions utilisées dans les articles abrogés mentionnés précédemment, à savoir celle au 2° et 3° du II de l'article 1er de l'ordonnance n° 2005-1516 sont abrogées.

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

Périmètre organique

Le projet de loi vise, comme le prévoit la directive, à assujettir les opérateurs de service essentiel (OSE) à la transposition NIS 2 en leur conférant le statut d'entité essentielle (EE).

Périmètre technique

La notion de système d'information essentiel est abandonnée au profit d'une application large des mesures de sécurité de l'opérateur de service essentiel (devenu EE) à l'ensemble de ses systèmes d'information, que ces derniers supportent le service pour lequel l'opérateur a été désigné comme OSE ou non.

En revanche, l'OSE, devenu EE, dispose d'une capacité à exempter certains de ses systèmes d'information de l'application des mesures de sécurité dès lors qu'il justifie que ces systèmes d'information ne génèrent aucun risque de dégradation ou d'interruption de ses activités ou services.

Mesures de sécurité

NIS 2 se présentant comme une réglementation cyber de masse, l'objectif est de définir un socle commun de cybersécurité visant à protéger les entités devant l'appliquer des principales menaces d'origines cybercriminelle et de masse (par exemple : les attaques par rançongiciels qui paralysent le système d'information, et par conséquent les activités de la victime jusqu'au versement d'une rançon à l'attaquant).

Dans le cadre de la simplification réglementaire, chaque réglementation liée à la cybersécurité nouvellement créée ou chaque réglementation liée à la cybersécurité existante faisant l'objet d'une mise à jour devrait s'appuyer sur ce socle commun de cybersécurité. Chaque réglementation pourra compléter ce socle de mesures spécifiques permettant d'atteindre les finalités visées par le texte.

2.2.3. Code de la défense

Les modifications du code de la défense visent à adapter la rédaction de ces articles au regard des dispositions du projet de loi (par exemple : les OIV et les OSE mentionné aux L. 2321-2-1 et L. 2321-3 sont remplacés par la notion d'entités essentielles prévues par la transposition de la directive NIS2.

3. OPTIONS POSSIBLES ET DISPOSITIF RETENU

3.1. OPTIONS ENVISAGEES

Aucune autre option n'a été envisagée.

3.2. DISPOSITIF RETENU

3.2.1. Ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives

En supprimant le raccrochement du RGS à l'article 9 de l'ordonnance n° 2005-1516 et en le couvrant via les dispositions du troisième alinéa de l'article 16 du projet de loi, les dispositions du I. de l'article 39 du projet de loi permettent de :

1) Modifier le champ d'application du RGS pour ne couvrir que les administrations visées par la transposition de la directive NIS 2.
2) Définir des mesures de sécurité spécifiques, pour les systèmes d'information supportant des échanges par voie électronique entre l'administration mettant en œuvre un tel système et les usagers de ce système d'information ou d'autres administrations, visant à limiter la fraude liée à l'usage de ces systèmes d'information.

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

La directive n° 2022/2555 dite « NIS 2 » abroge les dispositions de la directive NIS 1. Par conséquent, le projet de loi transposant la directive NIS 2, abroge les dispositions de la loi n° 2018-133 du 26 février 2018 (articles 1 à 15) transposant la directive NIS 1.

3.2.3. Modification de certaines dispositions du code de la défense

Les articles L. 2321-2-3 et L. 2321-3 du code de la défense (Chapitre I^{er}, titre II du livre III, deuxième partie) sont modifiés afin de remplacer la notion d'opérateur de service essentiel (OSE), par celle d'entité essentielle. Cette modification découle presque mécaniquement de l'abrogation de la directive NIS 1 et de la transposition de la directive NIS 2. A ce titre, elle n'emporte pas d'impacts distincts de ceux induits par la mise en œuvre du dispositif mis en place par NIS 2.

4. ANALYSE DES IMPACTS DES DISPOSITIONS ENVISAGEES

4.1. IMPACTS JURIDIQUES

4.1.1. Impacts sur l'ordre juridique interne

Les articles 1 à 15 de 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 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives sont abrogés.

S'agissant 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, les 2° et 3° de l'article 1er sont abrogés, les articles 9 et 12 sont abrogés et le I de l'article 14 est abrogé.

Les articles L. 2321-2-1 et L. 2321-3 du code de la défense sont modifiés.

4.1.2. Articulation avec le droit international et le droit de l'Union européenne

Sans objet.

4.2. IMPACTS ECONOMIQUES ET FINANCIERS

4.2.1. Impacts macroéconomiques

Pour l'économie et la société françaises, le passage de la directive NIS 1 à la directive NIS 2 permettra d'atteindre un niveau de sécurité renforcé pour adresser la cybercriminalité de masse, qui aura nécessairement pour effets de complexifier la tâche des attaquants et de diminuer, à leurs yeux, l'attrait des entités régulées. L'application de la réglementation NIS 2 permettra en effet de limiter la probabilité et la durée des interruptions de service, et donc la perte de chiffre d'affaires, voire le risque de faillite pour les organisations.

L'augmentation du niveau de sécurisation des acteurs économiques constitue également un facteur de compétitivité, dans la mesure où les donneurs d'ordres s'orientent plus volontiers vers des producteurs ou des prestataires dont la maitrise des moyens de production inspire confiance. Cela procure en effet des garanties en termes de disponibilité et donc de respect des délais contractuels, de protection des données, potentiellement stratégiques, confiées dans le cadre d'une prestation, et de fiabilité dans le résultat produit, la vulnérabilité des moyens de production à une attaque cyber pouvant aboutir à la corruption des produits livrés.

4.2.2. Impacts sur les entreprises

Ordonnance 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives

Un impact économique positif bénéficiera aux prestataires de services de confiance dont la qualification au titre du règlement eIDAS leur permettra d'être conforme aux exigences du RGS, les dispensant ainsi de s'engager dans un second processus de qualification au titre du RGS long et onéreux.

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

La suppression des dispositions relevant de la transposition de NIS 1 n'a pas d'impact autre que celui évoqué par ailleurs de l'application de NIS 2.

4.2.3. Impacts budgétaires

Sans objet.

4.3. IMPACTS SUR LES COLLECTIVITES TERRITORIALES

La modification des dispositions de l'ordonnance n° 2005-1516 aura un impact positif pour les collectivités territoriales puisqu'elle permettra de limiter les fraudes liées à l'usage de leurs services numériques telles que l'usurpation d'identité en ligne.

En outre, le socle commun d'exigences de sécurité, établi au titre de la transposition de la directive NIS 2, sur lequel s'appuie le RGS, permettra de rationaliser les coûts de sécurisation des systèmes d'information.

4.4. IMPACTS SUR LES SERVICES ADMINISTRATIFS

4.4.1. Ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives

La modification des dispositions de l'ordonnance n° 2005-1516 aura un impact positif pour les administrations. D'une part grâce à la simplification du cadre réglementaire qui leur est applicable, d'autre part en permettant de limiter les fraudes liées à l'usage des services numériques des administrations telles que l'usurpation d'identité en ligne.

Un impact financier positif est identifié pour les administrations puisque le socle commun d'exigences de sécurité, établi au titre de la transposition de la directive NIS 2, sur lequel s'appuie le RGS, permettra de rationaliser les coûts de sécurisation des systèmes d'information.

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

La suppression des dispositions relevant de la transposition de NIS 1 n'a pas d'impact autre que celui évoqué par ailleurs de l'application de NIS 2.

4.5. IMPACTS SOCIAUX

4.5.1. Impacts sur la société

Sans objet.

4.5.2. Impacts sur les personnes en situation de handicap

Sans objet.

4.5.3. Impacts sur l'égalité entre les femmes et les hommes

Sans objet.

4.5.4. Impacts sur la jeunesse

Sans objet.

4.5.5. Impacts sur les professions réglementées

Sans objet.

4.6. IMPACTS SUR LES PARTICULIERS

La révision du RGS devrait contribuer à renforcer la confiance des usagers dans l'usage des services numérique de l'administration.

4.7. IMPACTS ENVIRONNEMENTAUX

Sans objet.

5. CONSULTATIONS ET MODALITES D'APPLICATION

5.1. CONSULTATIONS MENEES

Conformément aux dispositions de l'article L. 1212-2 du code général des collectivités territoriales, la présente disposition a été soumise à l'examen du Conseil national d'évaluation des normes (CNEN) qui a rendu un avis défavorable le 22 mai 2024.

Enfin, sur le fondement de l'article 8 de la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, la Commission nationale de l'informatique et des libertés (CNIL) a été consultée à titre facultatif.

5.2. MODALITES D'APPLICATION

5.2.1. Application dans le temps

Ces dispositions entrent en vigueur au lendemain de la publication de la loi au *Journal officiel* de la République française. Néanmoins, l'abrogation des dispositions de la loi n° 2018-133 et

de l'ordonnance n° 2005-1516 seront effectives au moment de la publication des textes d'applications prévues respectivement aux articles 14 relatif aux mesures de sécurité NIS 2) et 16 (mesures spécifiques pour le RGS) du projet de loi.

5.2.2. Application dans l'espace

Conformément à l'article 40 du présent projet de loi, le titre II est applicable dans les îles Wallis et Futuna, en Polynésie française, en Nouvelle-Calédonie et dans les Terres australes et antarctiques françaises, sous réserve des adaptations suivantes :

1° 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, applicables localement.

2° Dans les îles Wallis et Futuna, en Polynésie française et en Nouvelle-Calédonie, les sanctions pécuniaires encourues en vertu du titre II de la présente loi sont prononcées en monnaie locale, compte tenu de la contre-valeur de l'euro dans cette monnaie.

Pour l'application du titre II à Saint-Barthélemy, Saint-Pierre-et-Miquelon, dans les îles Wallis et Futuna, en Polynésie française, en Nouvelle-Calédonie et dans les Terres australes et antarctiques françaises, les références à la directive (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 et aux règlements de l'Union européenne sont remplacées par la référence aux règles en vigueur en métropole en vertu de la même directive et des mêmes règlements.

L'article 16 de l'ordonnance du 8 décembre 2005 est modifié pour l'application dans les îles Wallis et Futuna.

Le I de l'article 24 de la loi du 26 février 2018 susvisée est modifié pour l'application à Wallis-et-Futuna, en Polynésie française, en Nouvelle-Calédonie et dans les Terres australes et antarctiques françaises.

5.2.3. Textes d'application

Les présentes dispositions ne requièrent aucun texte d'application.

Article 39 (IV) - Abrogation de la transposition de la directive NIS 1 et simplification du cadre réglementaire

1. ÉTAT DES LIEUX

1.1. CADRE GENERAL

La directive 2022/2555 dite NIS 2, dont l'objectif est d'assurer un niveau élevé commun de cybersécurité, portée par la présidence française de l'Union européenne, vise à répondre d'une part aux évolutions des menaces cyber et à leur augmentation (+255 % d'attaques aux rançongiciels en un an[192]) et d'autre part aux limites du cadre juridique existant.

Dès 2016, la directive 2016/1148 dite NIS 1 a imposé aux Etats membres de prendre des mesures afin d'assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information. Cette directive a été transposée en droit interne par la loi n° 2018-133 du 26 février 2018. L'article 23 de la directive NIS obligeait la Commission à revoir fréquemment les dispositions pour s'adapter aux évolutions en matière de cybersécurité. Au-delà de la menace stratégique (étatique) qui perdure, les cybercriminels ont élargi leur champ d'action à l'ensemble du tissu social et économique (PME, collectivités territoriales, hôpitaux…), avec parfois des conséquences extrêmement dommageables pour nos concitoyens. Le coût des cyberattaques ne cesse d'augmenter et a atteint, en 2022, 2 milliards d'euros en France avec un montant moyen de 58 600 euros par attaque[193].

Il est apparu que les réseaux de communications électroniques étaient particulièrement sensibles à ces attaques en raison de leur rôle central dans les communications, le partage d'information et l'usage d'internet. C'est pourquoi, les réseaux télécoms ont été introduits dans le champ d'application de la directive NIS 2 (article 2) de même que les offices d'enregistrement de noms de domaine. En fonction de leur taille et leur importance, ces opérateurs seront ensuite classés comme entité essentielle ou importante. De cette classification, la directive NIS 2, base du présent article, fait découler plusieurs obligations à la centaine d'opérateurs de réseaux de communications électronique comme la mise en place un cadre de gestion des risques ou l'harmonisation des modalités de remontée des incidents.

Si la transposition de NIS 2 implique majoritairement des modifications du code de la défense, elle a également un impact non négligeable sur le code des postes et des communications électroniques (CPCE) du fait de l'intégration des réseaux télécoms.

[192] ANSSI, Etat de la menace rançongiciel à l'encontre des entreprises et des institutions, 2021.

[193] BNP Paribas Entreprises, Cyberattaque : combien ça vous coûte concrètement, 2023.

1.1.1. Mesures de coordination

L'article L. 33-1 du CPCE impose aux opérateurs de communication électronique de déclarer tout incident affectant leurs réseaux. Un guide produit par le commissariat aux communications électroniques de défense (CCED) précise la marche à suivre pour que les opérateurs s'acquittent de cette obligation légale. Afin d'assurer la résilience des réseaux européens, dont les communications électroniques sont une composante essentielle, la directive NIS2 revoit les modalités de signalement des incidents par les entités essentielles en abrogeant les articles 40 et 41 de la directive 2018/1972 établissant un code des communications électroniques européen (CECE).

1.1.2. Systèmes de noms de domaine (DNS)

Le nom de domaine constitue l'adresse d'un site internet. Il est donc un élément central de la « toile ». Techniquement, il consiste dans une chaîne de caractère structurée, permettant la localisation et l'accès à un site internet, en évitant le recours à l'adresse IP (Internet Protocol) de celui-ci. L'adresse IP est formée d'une suite de chiffres qui identifie un ordinateur connecté au réseau ; le nom de domaine permet d'accéder très simplement au site internet qui est hébergé par l'ordinateur en cause, sans avoir recours à son adresse IP

En application de l'article L. 45 du code des postes et des communications électroniques les noms de domaine de l'internet correspondant aux codes pays du territoire national ou d'une partie de celui-ci doivent être enregistrés auprès d'un office d'enregistrement de premier niveau, l'Association française pour le nommage internet en coopération (AFNIC)[194], qui agit sur délégation du ministre chargé des communications électroniques. Cette obligation ne s'impose qu'aux noms de domaine nationaux et exclut notamment certains noms de domaine propres aux territoires d'outre-mer comme la Nouvelle-Calédonie ou la Polynésie française qui bénéficient de leur propre indice (.nc et .pf) en raison de leurs compétences propres en la matière. La réglementation de ces DNS n'est pas prévue par le CPCE.

Afin d'harmoniser les règles à l'échelle européenne et de pouvoir accéder aux données permettant d'identifier le propriétaire d'un nom de domaine en cas d'incident, l'article 28 de la directive NIS 2 prévoit de nouvelles règles en matière d'enregistrement des noms de domaine. Les Etats membres doivent imposer aux offices d'enregistrement de collecter et de conserver certaines données d'enregistrement des noms de domaine (nom du titulaire, point de contact, nom du domaine…) et organise l'accès et la publicité de ces données. La directive prévoit également que les Etats membres doivent prendre des mesures pour s'assurer de la

[194] Arrêté du 20 septembre 2021 désignant l'office d'enregistrement chargé d'attribuer et de gérer les noms de domaine au sein des domaines de premier niveau du système d'adressage par domaines de l'internet correspondant au « .fr **».**

fiabilité des serveurs et des bases de données des offices d'enregistrement des noms de domaine.

1.2. CADRE CONSTITUTIONNEL

Aux termes de l'article 88-1 de la Constitution : « La République participe aux Communautés européennes et à l'Union européenne, constituées d'Etats qui ont choisi librement, en vertu des traités qui les ont instituées, d'exercer en commun certaines de leurs compétences ». Le Conseil constitutionnel déduit de cette disposition que : « la transposition en droit interne d'une directive communautaire résulte d'une exigence constitutionnelle » (CC, n° 2004-496 DC du 10 juin 2004, Loi pour la confiance dans l'économie numérique)

L'article 74 de la Constitution prévoit que les modalités d'application des lois dans les collectivités d'outre-mer reposent sur une loi organique. En modifiant l'applicabilité des mesures dans les collectivités d'outre-mer, la présente disposition s'inscrit dans ce cadre constitutionnel et devra, à ce titre, veiller à sa compatibilité avec le statut qui régit chaque collectivité sous peine de censure (CC n° 80-122 DC, 22 juillet 1980, *Loi rendant applicable le Code de procédure pénale et certaines dispositions législatives dans les territoires d'outre-mer).*

Les mesures envisagées respectent également l'objectif de valeur constitutionnelle, d'accessibilité et intelligibilité du droit, principe consacré par la décision n° 99-421 DC du 16 décembre 1999 du Conseil constitutionnel, qui implique que les règles de droit doivent être claires, précises et compréhensibles par tous puisqu'elles permettent d'assurer la coordination et la mise à jour entre les dispositions connexes des différents codes.

En ce qui concerne particulièrement les noms de domaine, le conseil constitutionnel dans sa décision 2010-45 QPC a estimé que l'encadrement, tant pour les particuliers que pour les entreprises, du choix et de l'usage des noms de domaine sur internet affecte les droits de la propriété intellectuelle, la liberté de communication et la liberté d'entreprendre.

- S'agissant des droits de la propriété intellectuelle, leur rattachement à la protection constitutionnelle des articles 2 et 17 de la Déclaration de 1789 s'est fait en deux temps. Le Conseil a d'abord reconnu la protection la propriété industrielle et commerciale, en 1991 (90-283 DC du 8 janvier 1991). Dans un second temps, le Conseil a consacré l'extension de cette protection constitutionnelle aux droits de la propriété culturelle (2006-240 DC du 27 juillet 2006). Enfin le Conseil a précisé la portée de la protection constitutionnelle des droits d'auteur, compris comme « le droit, pour les titulaires du droit d'auteur et de droits voisins, de jouir de leurs droits de propriété intellectuelle et de les protéger dans le cadre défini par la loi et les engagements internationaux de la France » (2009-580 DC du 10 juin 2009). Dans la motivation de sa décision du 6

octobre 2010, le Conseil constitutionnel relève que l'encadrement du choix et de l'usage des noms de domaine affecte les droits de la propriété intellectuelle ;

- Dans sa décision n° 2008-580 DC, le conseil a consacré une valeur forte au droit d'accéder à l'internet comme un droit attaché à l'article 11 de la Déclaration des droits de l'homme et du citoyen de 1789 en jugeant « *qu'en l'état actuel des moyens de communication et eu égard au développement généralisé des services de communication au public en ligne ainsi qu'à l'importance prise par ces services pour la participation à la vie démocratique et l'expression des idées et des opinions, ce droit implique la liberté d'accéder à ces services* ». Il reprend ce raisonnement dans sa décision 2010-45 QPC et juge ainsi « *qu'en l'état actuel des moyens de communication et eu égard au développement généralisé des services de communication au public en ligne ainsi qu'à l'importance prise par ces services dans la vie économique et sociale, notamment pour ceux qui exercent leur activité en ligne, l'encadrement, tant pour les particuliers que pour les entreprises, du choix et de l'usage des noms de domaine sur internet affecte la liberté de communication et la liberté d'entreprendre.* » La référence à la liberté d'entreprendre, qui découle de l'article 4 de la Déclaration de 1789, vient ainsi s'ajouter à la liberté de communication.

Dans la même décision 2010-45 QPC le conseil constitutionnel reconnait par ailleurs que le législateur doit sur la base de l'article 34 de la Constitution déterminer « *les principes fondamentaux (…) des obligations civiles et commerciales* ». Il précise que « *ressortissent en particulier aux principes fondamentaux de ces obligations civiles et commerciales les dispositions qui mettent en cause leur existence même* ». Il reconnait ainsi une obligation du législateur de fixer des principes généraux pour définir les conditions dans lesquelles les noms de domaine sont attribués ou peuvent être renouvelés, refusés ou retirés.

1.3. CADRE CONVENTIONNEL

Le présent article vise à transposer les mesures issues de la directive 2022/2555 dite NIS 2 en matière de signalement des incidents et d'encadrement de l'enregistrement des noms de domaine. Plus largement, elle s'inscrit dans la stratégie de l'Union européenne pour renforcer la résilience des organisations essentielles au sein de l'Union qui a abouti aux directives n° 2022/2557 dite « REC », concernant la résilience des entités critiques, et n° 2022/2556 dite DORA concernant la résilience opérationnelle numérique du secteur financer.

1.4. ÉLEMENTS DE DROIT COMPARE

1.4.1. En matière de cybersécurité

La hausse des menaces cyber ne touche pas que l'Europe. Plusieurs pays se sont ainsi dotés de législations en matière de cybersécurité pour faire face à ces nouvelles menaces. Le Royaume-Uni a développé une stratégie nationale de cybersécurité en 2022. Cette stratégie ne concerne cependant que les organisations gouvernementales et vise à la fois à renforcer la protection face aux risques cyber mais aussi la résilience en cas d'incident[195]. De même, les Etats-Unis ont engagé une stratégie de cybersécurité en 2023 qui est similaire à la directive NIS 2. En effet, les autorités américaines ont souhaité renforcer les exigences obligatoires qui pèsent sur les infrastructures critiques notamment les opérateurs de communications électroniques[196].

1.4.2. Sur les noms de domaine

Aux Etats-Unis et au Royaume-Uni, l'enregistrement des noms de domaine de premier niveau repose également sur une organisation unique qui reçoit une délégation pour fournir les noms de domaine (Nominet au Royaume-Uni et Neustar aux Etats-Unis). Les règles d'acquisition sont sensiblement similaires avec une obligation de résidence ou d'exercice d'une activité sur le territoire de l'Etat.

2. OBJECTIFS POURSUIVIS ET NECESSITE DE LEGIFERER

2.1. OBJECTIFS POURSUIVIS

L'objectif poursuivi est de mettre en conformité le droit interne avec la directive NIS 2 concernant la cybersécurité. Au-delà de cette obligation juridique, cet article permet d'adapter les dispositions du CPCE relatives aux modalités d'enregistrement des noms de domaine de premier niveau. L'article vise enfin à répondre aux objectifs d'intelligibilité et de clarté de la loi en harmonisant les dispositions du CPCE avec celles du présent projet de loi.

2.2. NECESSITE DE LEGIFERER

Si des dispositions existent dans le droit national, particulièrement dans le CPCE, ces dernières ne permettent pas d'assurer entièrement la transposition des mesures imposées par la directive NIS 2. La transposition des directives est une obligation à valeur constitutionnelle (n° 2004-496 DC du 10 juin 2004, « Loi pour la confiance dans l'économie numérique ») et celle-ci doit être effectuée avant le 17 octobre 2024. La nécessité de légiférer découle donc directement de l'adoption de la directive NIS 2.

[195] National cyber strategy, UK, 2022.

[196] National cybersecurity strategy, USA, mars 2023.

De plus, les mesures relatives aux obligations de déclaration des incidents et celles portant sur l'enregistrement des noms de domaine sont de nature législative ce qui oblige à légiférer afin d'assurer l'harmonisation du CPCE avec les mesures de la directive NIS 2 ainsi que les évolutions induites par le projet de loi résilience.

3. OPTIONS POSSIBLES ET DISPOSITIF RETENU

3.1. OPTIONS ENVISAGEES

Aucune autre option n'a été envisagée.

3.2. DISPOSITIF RETENU

Le IV du présent article vise à remplacer la mention de la déclaration des incidents prévue à l'article L. 33-1 par un r) faisant référence au présent projet de loi. L'objectif est ainsi de supprimer, au sein du CPCE, les dispositions spéciales concernant la cybersécurité en matière de communications électroniques afin de les intégrer dans le droit général prévu par le projet de loi résilience.

L'abrogation des articles 40 et 41 de la directive CECE rend nécessaire de remplacer les références à cette directive dans le CPCE par une référence à la présente loi qui devient la loi spécifique en matière de cybersécurité notamment par la création d'un r) au I de l'article L. 33-1 du CPCE précisant que les obligations de la présente loi sont applicables aux opérateurs de communications électroniques pour la fourniture de leurs services.

Certains articles du CPCE sont modifiés pour enlever la référence à l'obligation de notification imposée aux opérateurs de communications électroniques (L. 33-1) ainsi que pour préciser les modalités de communication des données collectées par les offices d'enregistrement. Ces suppressions n'auront qu'un impact réduit sur les opérateurs puisqu'elles sont remplacées par des obligations au titre du présent projet de loi.

Enfin, les articles L. 45-4 et L. 45-5 précisent les éléments que doit contenir le décret en Conseil d'Etat, prévu à l'article L. 45-7, visant à assurer l'application des mesures législatives relatives à l'enregistrement des noms de domaine. En ce sens, le présent article rend nécessaire une modification du décret n° 2015-1317 du 20 octobre 2015 pris en application des articles L. 33-6 et L. 45 du code des postes et des communications électroniques.

4. ANALYSE DES IMPACTS DES DISPOSITIONS ENVISAGEES

4.1. IMPACTS JURIDIQUES

4.1.1. Impacts sur l'ordre juridique interne

Des articles du CPCE nécessitent un ajustement sans modification majeure de l'architecture du code. Les articles modifiés sont les articles : L. 33-1 ; L. 45 ; L. 45-3 ; L. 45-4 ; L. 45-5 et L. 45-8.

4.1.2. Articulation avec le droit international et le droit de l'Union européenne

Les modifications prévues par le présent dispositif permettront de se mettre en conformité avec les dispositions la directive NIS 2 et de la rendre pleinement effective en droit interne. Le présent article vise donc expressément à assurer l'articulation du droit interne avec le droit de l'Union européenne.

4.2. IMPACTS ECONOMIQUES ET FINANCIERS

4.2.1. Impacts macroéconomiques

Sans objet.

4.2.2. Impacts sur les entreprises

La modification prévue de l'article L. 33-1 du CPCE rend applicable, en droit interne, aux opérateurs de télécommunication, l'ensemble des dispositions prévues par le projet de loi résilience. A ce titre, cette norme aura un impact sur les opérateurs de communications électroniques qui devront se mettre en conformité avec les dispositions envisagées.

Cependant, la mesure proposée permettra de renforcer la résilience des opérateurs et de les protéger des incidents ce qui réduira d'autant les risques d'attaque cyber et donc les coûteux impacts qui en résultent.

4.2.3. Impacts budgétaires

Sans objet.

4.3. IMPACTS SUR LES COLLECTIVITES TERRITORIALES

Sans objet.

4.4. IMPACTS SUR LES SERVICES ADMINISTRATIFS

Sans objet.

4.5. IMPACTS SOCIAUX

Sans objet.

4.5.1. Impacts sur la société

Sans objet.

4.5.2. Impacts sur les personnes en situation de handicap

Sans objet.

4.5.3. Impacts sur l'égalité entre les femmes et les hommes

Sans objet.

4.5.4. Impacts sur la jeunesse

Sans objet.

4.5.5. Impacts sur les professions réglementées

Sans objet.

4.6. IMPACTS SUR LES PARTICULIERS

Sans objet.

4.7. IMPACTS ENVIRONNEMENTAUX

Sans objet.

5. CONSULTATIONS ET MODALITES D'APPLICATION

5.1. CONSULTATIONS MENEES

Conformément aux dispositions de l'article L. 1212-2 du code général des collectivités territoriales, la présente disposition a été soumise à l'examen du Conseil national d'évaluation des normes (CNEN) qui a rendu un avis défavorable le 22 mai 2024.

En application de l'article L. 36-5 du code des postes et des communications électroniques, le présent article a été soumis à l'examen de l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse (ARCEP). Le 23 mai 2024, elle a rendu un avis n° 2024-1131 favorable au renforcement des mesures visant à assurer un niveau élevé de cybersécurité. Il appelle également à prévoir un délai suffisant aux acteurs pour se mettre en conformité, des critères de désignation des entités suffisamment précis ainsi qu'une bonne articulation de ces nouvelles obligations avec les dispositions du code de la défense pour les opérateurs d'importance vitale.

Enfin, sur le fondement de l'article 8 de la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, la Commission nationale de l'informatique et des libertés (CNIL) a été consultée à titre facultatif.

5.2. MODALITES D'APPLICATION

5.2.1. Application dans le temps

La disposition entrera en vigueur le lendemain de la publication de la loi au *Journal officiel* de la République française.

5.2.2. Application dans l'espace

L'article est applicable de plein droit dans les départements relevant de l'article 73 de la Constitution (Guadeloupe, Guyane, Martinique, Mayotte, La Réunion).

Il est également applicable dans les collectivités de Saint-Barthélemy, Saint-Martin, Saint-Pierre-et-Miquelon eu égard à leurs lois organiques respectives.

Le présent article rend également applicable les dispositions relatives à l'enregistrement des noms de domaine dans leur nouvelle rédaction aux îles Wallis et Futuna et aux Terres australes et antarctiques françaises.

5.2.3. Textes d'application

Des modifications du décret n° 2015-1317 du 20 octobre 2015 pris en application des articles L. 33-6 et L. 45 du code des postes et des communications électroniques seront nécessaires pour tenir compte des précisions introduites par le présent article aux articles L. 45-4 et L. 45-5 du CPCE.

Article 40 – Mesures applicables à l'outre-mer pour les territoires sous spécialité législative

1. ÉTAT DES LIEUX

1.1. CADRE GENERAL

La menace cybercriminelle de masse se généralise et se professionnalise depuis plusieurs années, ce qui se traduit concrètement par un nombre croissant de victimes de cyberattaques dans tous les secteurs d'activité, publics et privés et impactant notamment les collectivités territoriales.

L'Union européenne a déjà pris conscience de la nécessité de protéger de la menace cyber les acteurs du marché unique, afin de limiter les impacts économiques, financiers et sociétaux de la cybercriminalité, en élaborant la directive 2016/1148 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", premier instrument du marché intérieur visant à améliorer la résilience de l'UE contre les risques liés à la cybersécurité.

Cette directive européenne a été transposée en droit français au moyen de la loi n° 2018-133 du 26 février 2018 portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité.

La réglementation désormais en vigueur, communément appelée NIS (*Network and Information Security*) 1, concerne aujourd'hui les six secteurs d'activité que l'UE avait jugés prioritaires de par leurs effets potentiellement systémiques (Energie, Transports, Banque et marchés financiers, Santé, Eau potable, Infrastructures numériques), auxquels la France a ajouté six autres secteurs qu'elle a estimés à enjeux également prioritaires (Assurance, Restauration, Traitement des eaux, Education, Emploi et formation, Organismes sociaux).

Dans le cadre de la transposition de la directive NIS 1, les mesures ont été étendues aux pays et territoires d'outre-mer (PTOM). Ces territoires insulaires, malgré leur taille modeste et leur faible poids démographique, disposent de la majorité des services essentiels. Cependant, ces spécificités ainsi que l'éloignement de la métropole ont pu rendre moins aisées l'identification des opérateurs pour l'ensemble de ces services essentiels et leur désignation.

Le texte de la première directive NIS prévoyait que la Commission européenne réexamine périodiquement le fonctionnement global de la directive et évalue la liste des secteurs et sous-secteurs dans lesquels sont identifiés des opérateurs de services essentiels et les types de services numériques couverts par la directive. C'est dans le respect de cet engagement que la nouvelle directive (n° 2022/2555, appelée "NIS 2") a été élaborée. Son évolution de périmètre

confirme aujourd'hui au niveau européen ce que la France avait anticipé en 2018, en intégrant certains des secteurs d'activité qui avaient été pris en compte au niveau national en 2018. Elle pose également le principe de couvrir également les collectivités territoriales, en fonction de l'organisation interne de chacun des pays membres.

1.2. CADRE CONSTITUTIONNEL

La Constitution énumère les collectivités situées outre-mer (art. 72-3) et détermine leur régime juridique (art. 72-3, 73 et 74). Elle distingue :

- **les collectivités régies par son article 73** : département de Guadeloupe, de la Réunion, région de la Guadeloupe et de la Réunion, les collectivités de la Guyane, de la Martinique et de Mayotte ;
- **les collectivités régies par son article 74** : Saint-Barthélemy, Saint-Martin, Saint-Pierre-et Miquelon, Wallis et Futuna, la Polynésie française ;
- Les Terres australes et antarctiques françaises et l'Ile de Clipperton **régies par l'article 72-3 alinéa 4 ;**
- la Nouvelle Calédonie qui relève de son **titre XIII, article 76 et 77.**

Deux régimes législatifs coexistent :

- **le régime de l'identité législative** : les lois et règlements nationaux sont applicables de plein droit dans les collectivités concernées. Pour tenir compte des spécificités ultramarines, des adaptations sont néanmoins possibles mais le titre II du projet de loi n'en prévoit pas. Il s'agit :
    - des collectivités de l'article 73 ;
    - de Saint-Barthélemy[197], Saint-Pierre-et-Miquelon[198] et Saint Martin[199] dont les statuts prévoient que la plupart des lois et règlements y sont applicables de plein droit (sauf celles intervenant dans les matières qui relèvent de la loi organique).

Dès lors, pour ces collectivités, les dispositions du titre II s'applique de plein droit, ne contiennent aucune adaptation et n'impliquent aucune consultation.

[197] Article LO. 6213-1 du code général des collectivités territoriales (CGCT).

[198] Article LO. 6413-1 du CGCT.

[199] Article LO. 6313-1 du CGCT.

- **le régime de spécialité législative** : seules les dispositions législatives et réglementaires qui comportent une mention expresse à cette fin sont applicables dans ces territoires, sauf pour les domaines relevant statutairement des compétences de l'Etat applicables de plein droit. Effectivement, pour ces collectivités, **une loi organique définit leur statut particulier** : pour la Nouvelle-Calédonie, la Polynésie française, les **Terres australes et antarctiques françaises (TAAF) et Wallis et Futuna. Le titre II du projet de loi qui traite de la sécurité des systèmes d'information touche au domaine de la défense nationale. Or en matière de défense nationale, l'Etat est compétent pour les lois et règlements intervenant dans ce domaine, qui sont applicables de plein droit** :
    - En **Nouvelle-Calédonie**, cette compétence est prévue par le 2° de l'article 21 de la loi organique de la loi organique n° 99-209 du 19 mars 1999, qui définit les compétences de l'Etat dans cette collectivité. Or, par dérogation au principe de spécialité législative, les lois et règlements de l'Etat sont applicables de plein droit dans le domaine de la défense nationale (article 6 2° de la loi organique).
    - En **Polynésie française**, cette compétence est prévue en application du 4° de l'article 14 de la loi organique n° 2004-192 du 27 février 2004, article qui liste les compétences de l'Etat dans cette collectivité. De même, par dérogation au principe de spécialité législative, les lois et règlements de l'Etat sont applicables de plein droit dans le domaine de la défense nationale (article 7 2° de la loi organique).
    - Pour les **TAAF**, cette compétence est prévue au 2° de l'article 1-1 de la loi n° 55-1052 du 6 aout 1955 qui a prévu une application de plein droit des dispositions législatives et règlementaires en matière de défense nationale.
    - Dans les **îles Wallis et Futuna**, jusqu'à l'intervention des dispositions organiques prévues par l'article 74 de la Constitution, le régime législatif et règlementaire des îles Wallis et Futuna est déterminé par (i) la loi n°61-814 du 29 juillet 1961 modifiée, conférant aux îles Wallis et Futuna le statut de territoire d'outre-mer; (ii) le décret n° 57-811 du 22 juillet 1957 relatif aux attributions de l'assemblée territoriale, du conseil territorial et de l'administrateur supérieur des îles Wallis et Futuna.

Seules les lois de souveraineté sont d'application de plein droit dans cette collectivité et le Conseil d'Etat semble rattacher l'ensemble de la défense nationale à la catégorie des lois de souveraineté [Conseil d'État, avis section de l'administration n° 398850 du 26 novembre 2019]. De plus, le décret précité liste, en son article 40, les domaines dans lesquels l'assemblée de Wallis et Futuna prend des délibérations portant réglementation territoriale et parmi les 41 items, aucun ne concerne, les domaines visés par le titre II du projet de loi.

Aussi, par dérogation au principe de spécialité législative, les lois et règlement de l'Etat sont applicables de plein droit (article 4 de la loi précitée).

Ainsi, l'analyse des statuts de chacune de ces collectivités ou territoires, permet d'établir que les dispositions qui relèvent de la compétence de défense de l'Etat sont en principe applicables de plein droit.

1.3. CADRE CONVENTIONNEL

Le cadre constitutionnel est à envisager en lien avec le droit de l'UE en la matière.

En effet, le titre II du projet de loi vise à transposer ou adapter dans notre droit national, les textes européens suivants :

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

En ce qui concerne les collectivités et territoires de la France, le traité sur le fonctionnement de l'Union européenne (TFUE) distingue :

- les régions ultrapériphériques – RUP (article 349 du TFUE) ;
- les pays et territoires d'outre-mer – PTOM (article 355 TFUE).

Collectivités et territoires	Statut en droit de l'UE (TFUE)	Droit de l'UE directement applicable
La Réunion La Guadeloupe La Guyane française	RUP – article 349 TFUE	OUI

La Martinique Mayotte Saint-Martin		
Saint-Barthélemy Saint-Pierre-et-Miquelon La Nouvelle-Calédonie La Polynésie française Les terres australes et antarctiques Les îles Wallis et Futuna	PTOM – article 355-2 TFUE	NON

Or, si l'ensemble du droit de l'Union européenne, primaire comme dérivé, est applicable de plein droit dans les régions ultrapériphériques (RUP), il n'est pas applicable dans les pays et territoires d'outre-mer (PTOM). Il convient donc d'étendre les dispositions issues du droit de l'UE dans le respect de ce statut et des principes d'identité ou spécialité législative.

Effectivement, dans la mesure où les dispositions du titre II du projet de loi visent à adapter le droit national au droit de l'Union européenne, certaines de ces dispositions renvoient directement aux textes de droit dérivé précités (références, notions définitions ou des listes contenues dans les textes européens).

Ces références au droit de l'UE pourraient potentiellement trouver à s'appliquer dans les PTOM.

Il a donc été fait le choix, afin de respecter l'inapplicabilité du droit de l'UE dans ces territoires, de rendre applicables dans ces territoires les dispositions du titre II du projet de loi, « en tant que droit national faisant référence au droit dérivé ». Dans cette dernière hypothèse, la doctrine des sections administratives du Conseil d'État [CE avis du 26 février 2013, section des travaux publics, n° 387319, projet de loi DADDUE dans le domaine du développement durable ; CE avis du 7 juillet 2015, section des travaux publics, n°390154, projet de loi DADDUE dans le domaine de la prévention des risques] prévoit qu'il faut, d'une part, étendre explicitement la disposition nationale qui fait référence au droit de l'UE, par mise à jour d'un "compteur Lifou" et, d'autre part, prévoir une rédaction d'adaptation selon laquelle les dispositions de droit de l'UE ne sont étendues que pour les besoins de l'application des dispositions nationales qui y font référence.

Comme indiqué supra, une particularité s'ajoute s'agissant de Saint-Barthélemy et Saint-Pierre-et-Miquelon, lesquelles, bien que relevant en droit de l'UE de la catégorie des PTOM, sont régies en droit national par le principe de l'identité législative. Les dispositions nationales s'y appliquent ainsi de plein droit, selon le Conseil constitutionnel, y compris en ce qu'elles font référence à des normes de droit dérivé de l'UE [Cons. const. n° 2018-765 DC du 12 juin 2018, Loi relative à la protection des données personnelles]. Ainsi, pour la section des finances, les dispositions qui font référence au droit de l'UE s'appliquent de plein droit à ces collectivités sauf mention expresse contraire [Avis du CE 13 octobre 2020, section des finances, n°401046 projet de décret modifiant le code de la consommation en ce qui concerne les denrées alimentaires].

Ainsi :

- S'agissant de la Martinique, Mayotte, la Guadeloupe, la Guyane, la Réunion et de Saint-Martin, eu égard à leur statut de RUP au regard du droit de l'Union européenne et du principe d'identité législative qui leur est applicable, le titre II du projet de loi qui met en œuvre des textes européens y est donc applicable de plein droit.
- S'agissant de Saint-Barthélemy et Saint-Pierre-et-Miquelon (PTOM) les actes de droit dérivé de l'Union européenne n'y sont en principe pas applicables et les **renvois directs** au droit de l'UE ne sont pas possibles. Les dispositions du titre II du projet de loi y sont applicables, « en tant que droit national faisant référence au droit dérivé ».
- S'agissant de la Polynésie française, les îles Wallis et Futuna et la Nouvelle-Calédonie qui sont également des PTOM. Les textes européens ci-dessus visés ne sont pas applicables dans ce territoire et les **renvois directs** au droit de l'UE ne sont pas possibles. Les dispositions du titre II du projet de loi y sont applicables, « en tant que droit national faisant référence au droit dérivé ».

Enfin, l'article 13 du projet de loi en ce qu'il renvoie à des textes sectoriels non visés explicitement (existants ou à venir) ne peut être applicable au PTOM. Son inapplicabilité a été précisée à l'article 40 conformément aux principes d'identité et spécialité législative selon les collectivités et territoires.

1.4. ELEMENTS DE DROIT COMPARE

Sans objet.

2. OBJECTIFS POURSUIVIS ET NECESSITE DE LEGIFERER

2.1. OBJECTIFS POURSUIVIS

Les objectifs de la mesure sont les suivants :

- Définir le champ d'application des obligations portées par la loi. Définir en droit national le périmètre d'application dans les limites de latitude données aux Etats membres et inscrites dans la directive 2022/2555. Permettre à toutes les entités de comprendre dans quelles conditions et à quel titre elles sont concernées par la réglementation NIS 2, sur la base de critères clairement définis et de catégories auxquelles seront associés des niveaux d'exigence adaptés.
- Définir les articulations avec les réglementations nationales et sectorielles ayant également des impacts sur la cybersécurité, et préciser les conditions dans lesquelles certains opérateurs seront exclus de l'application de NIS 2 au titre notamment de clauses relatives à la sécurité nationale.
- Définir les conditions de régulation, les obligations et les dispositions qui seront mises en place pour que l'autorité nationale cyber et les entités assujetties à NIS 2 remplissent leurs obligations et en rendent compte.

2.2. NECESSITE DE LEGIFERER

La transposition en droit national doit intégrer les pays et territoires d'outre-mer (PTOM) ne faisant pas partie du territoire de l'UE (la Polynésie française, Wallis et Futuna, la Nouvelle-Calédonie, les Terres Australes et Antarctique Françaises, Saint-Pierre et Miquelon, Saint-Barthélemy) pour les raisons suivantes :

- Continuité et égalité territoriale entre l'Hexagone et les PTOM ;
- Cohérence avec la posture adoptée au moment de la transposition de la directive NIS 1. La menace s'amplifie et n'épargne pas les territoires d'outre-mer. Ces territoires sont de plus de plus en plus connectés et soumis aux attaques informatiques.

Pour mémoire, les autres territoires d'outre-mer (cinq départements et régions d'outre-mer[200] et Saint-Martin) font partie du territoire de l'Union européenne et seront soumis à la directive européenne NIS 2 dans les mêmes conditions que pour l'Hexagone.

Les dispositions législatives du titre II sont étendues aux territoires et collectivités d'outre-mer, dont certaines d'entre elles font référence aux textes européens, il est apparu nécessaire de prévoir un article de loi qui définit, dans le respect des compétences locales, des statuts de PTOM ou RUP et des principes d'identité et spécialité législative, les dispositions applicables à ces collectivités.

[200] Guadeloupe, Guyane, Martinique, Mayotte, La réunion.

3. OPTIONS ENVISAGEES ET DISPOSITIF RETENU

3.1. OPTIONS ENVISAGEES

L'obligation de transposition ne laisse pas envisager d'autres options.

3.2. DISPOSITIF RETENU

Pour chaque objectif poursuivi, les dispositifs retenus sont les suivants.

- En matière de périmètre d'application, le projet de loi prévoit une application sans restriction des éléments prescriptifs de la directive NIS 2 relatifs à la définition des entités concernées, aux critères et seuils, aux secteurs, sous-secteurs et types d'entité.
- Dans le cas du secteur privé, il est prévu d'intégrer les opérateurs implantés dans ces PTOM pour les secteurs d'activité listés dans la directive NIS 2. La répartition des entreprises dans les outre-mer montre que de nombreuses entreprises appartenant à ces secteurs critiques d'activités sont en-dessous des seuils définis par la directive. Compte tenu de la décision prise de ne pas définir de seuils spécifiques pour l'outre-mer, l'identification des entités régulées (essentielles/importantes) fera l'objet d'une désignation individuelle.
- Dans le cas du secteur des administrations, la transposition prévoit une déclinaison au niveau local, pour prendre en compte les conseils régionaux, les conseils départementaux, les intercommunalités, les grandes communes et les communautés de communes.

Afin de garantir la continuité et l'égalité territoriale entre l'Hexagone et les PTOM, cette déclinaison intégrera les « administrations centrales » de l'ensemble des PTOM :

- Gouvernement de Polynésie Française,
- Gouvernement de Nouvelle-Calédonie,
- Collectivité de Saint-Barthélemy,
- Circonscriptions territoriales de Wallis et Futuna (Ulvea, Alo, Sigave),
- Collectivité de Saint-Pierre & Miquelon,
- Les TAAF[201].

[201] Les TAAF ont la particularité de bénéficier à la fois du statut d'administration déconcentrée et de celui de collectivité d'outre-mer. Elles seront ainsi régulées par rapport à chacun de leurs statuts.

Il en sera de même pour les intercommunalités, les grandes communes et les communautés de communes de ces PTOM, dans les mêmes conditions que dans l'Hexagone.

Le projet de loi maintient le pouvoir de désignation exceptionnelle, par arrêté du Premier ministre, d'entités dont le niveau de criticité estimé en concertation avec les ministères coordonnateurs le justifie, sans considération des seuils de chiffre d'affaires ou de nombre d'employés applicables dans le cadre général.

4. ANALYSE DES IMPACTS DES DISPOSITIONS ENVISAGEES

4.1. IMPACTS JURIDIQUES

4.1.1. Impacts sur l'ordre juridique interne

Il est créé un article 40 dans le présent projet de loi visant à définir le régime applicable outre-mer qui ne sera pas codifié.

Les dispositions des I à III de l'article 40 visent à préciser l'applicabilité du titre II à l'outre-mer.

Les dispositions du IV à VII visent à coordonner les textes et à assurer la cohérence en l'outre-mer pour les textes respectifs suivants :

- la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique ;
- l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives ;
- 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.

L'ensemble du titre II à l'exception de l'article 13 est applicable à l'outre-mer.

4.1.2. Articulation avec le droit international et le droit de l'Union européenne

En ce qui concerne les collectivités et territoires de la France, le traité sur le fonctionnement de l'Union européenne (TFUE) distingue :

- les régions ultrapériphériques – RUP (article 349 du TFUE) ;
- les pays et territoires d'outre-mer – PTOM (article 355 TFUE).

Le titre II du projet de loi vise à transposer ou adapter dans notre droit national, les textes européens suivants :

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

4.2. IMPACTS ECONOMIQUES ET FINANCIERS

4.2.1. Impacts macroéconomiques

Sans objet.

4.2.2. Impacts sur les entreprises

Les territoires d'outre-mer disposent d'un tissu économique et de collectivités territoriales de plus en plus numérisés et connectés. L'isolement des territoires de par leur insularité et l'éloignement de l'hexagone se traduit par l'existence d'entités essentielles et importantes dans tous les secteurs et sous-secteurs de la directive NIS 2 : électricité, transports, banque et infrastructures de marchés financiers, infrastructures numériques, espace, services postaux et d'expédition, industrie manufacturière, transformation et distribution des denrées alimentaires, etc.

Ces acteurs essentiels sont de tailles plus modestes que dans l'hexagone en raison de la faiblesse du marché des territoires d'outre-mer. De plus, ces entreprises sont souvent des acteurs disposant de monopoles. En raison d'un sentiment de sécurité lié à l'insularité, la sensibilité au risque cyber s'avère plus faible que dans l'hexagone. Ces spécificités accroissent les vulnérabilités des territoires d'outre-mer, ce qui risque d'en faire des victimes de choix pour les attaquants.

L'augmentation du niveau de sécurisation des acteurs essentiels et importants sur l'hexagone avec la NIS 2 ne doit pas avoir pour conséquence un déport des cyberattaques vers les territoires d'outre-mer. Afin de réduire ce risque, la mise en œuvre de NIS 2 dans les DROM/COM doit se faire dans la même temporalité que sur l'hexagone. Cette mise en œuvre devra intégrer la désignation d'entités de tailles modestes en dessous des seuils définis par NIS 2 mais néanmoins essentielles et importantes à l'échelle de territoire concerné.

4.2.3. Impacts budgétaires

Sans objet.

4.3. IMPACTS SUR LES COLLECTIVITES TERRITORIALES

Pas d'impact sur les collectivités territoriales spécifique à l'outre-mer.

4.4. IMPACTS SUR LES SERVICES ADMINISTRATIFS / L'AUTORITE NATIONALE

Sans objet.

4.5. IMPACTS SOCIAUX

Sans objet.

4.6. IMPACTS SUR LES PARTICULIERS

Sans objet.

4.7. IMPACTS ENVIRONNEMENTAUX

Sans objet.

5. CONSULTATIONS ET MODALITES D'APPLICATION

5.1. CONSULTATIONS MENEES

Conformément aux dispositions de l'article L. 1212-2 du code général des collectivités territoriales, la présente disposition a été soumise à l'examen du Conseil national d'évaluation des normes (CNEN) qui a rendu un avis défavorable le 22 mai 2024.

Enfin, sur le fondement de l'article 8 de la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, la Commission nationale de l'informatique et des libertés (CNIL) a été consultée à titre facultatif.

5.2. MODALITES D'APPLICATION

5.2.1. Application dans le temps

Le présent article entre en vigueur le lendemain de la publication du présent projet de loi au *Journal officiel* de République française.

5.2.2. Application dans l'espace

La réglementation NIS 2 est applicable dans l'ensemble de l'Union européenne, et sera transposée à l'ensemble du territoire national. Des dispositions particulières sont prévues pour couvrir les collectivités territoriales à statut particulier (notamment Outre-mer) et selon le principe de spécialité législative.

5.2.3. Textes d'application

Le présent article ne requiert aucun mesure d'application.

CHAPITRE V – DISPOSITIONS RELATIVES AUX COMMUNICATIONS ELECTRONIQUES

Article 41 – Renforcement des sanctions pénales pour améliorer la lutte contre les brouillages

1. ÉTAT DES LIEUX

1.1. CADRE GENERAL

La transmission hertzienne, c'est-à-dire sur des liaisons sans fil (réseaux de téléphonie mobile, réseaux professionnels privés, WIFI, etc.) de données ou de la voix tient une place essentielle dans la continuité des activités économiques, sociétales et étatiques (à titre d'exemple, la couverture mobile des territoires, la connectivité des zones reculées, les services de surveillance à domicile de personnes âgées, les terminaux de paiement par carte, les appels d'urgence sur téléphone mobile, ou encore le fonctionnement des radars de prévisions météorologiques) et des infrastructures de la nation.

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.

Les conditions non conformes peuvent concerner :

- l'utilisation d'une fréquence sans l'autorisation nécessaire si c'est une fréquence soumise à autorisation individuelle (article L. 41.1 du CPCE) ou en dehors des conditions réglementaires si c'est une fréquence ne nécessitant pas d'autorisation individuelle (L. 33-3 du CPCE) - l'ANFR est en charge du contrôle ;
- L'utilisation d'une installation radioélectrique sans l'accord de l'ANFR (article L. 43 du CPCE) - l'ANFR est en charge du contrôle ;
- l'utilisation non conforme d'un équipement ou d'une installation radioélectrique qui au regard de la transposition en droit national de la directive des équipements radioélectriques (RED) qui impose que les équipements mis sur le marché suivent un certain nombre d'exigences essentielles (article L. 34-9 du CPCE) dont celle de ne pas causer de brouillage - l'ANFR est une autorité de contrôle pour la surveillance du marché des équipements radioélectriques ;

– l'utilisation d'un appareil, équipement ou installation électrique ou électronique non conforme en matière de compatibilité électromagnétique au regard de la directive Compatibilité Electromagnétique (directive CEM) qui exige que les équipements électriques et électroniques mis sur le marché européen respectent un certain nombre d'exigences essentielles dont celle de ne pas brouiller – la Direction générale de la Concurrence, de la Consommation et de la Répression des fraudes (DGCCRF) est une autorité de contrôle pour la surveillance du marché des équipements électriques et électroniques.

La lutte contre ces perturbations ou brouillages contribue ainsi au bon fonctionnement des services de communication par radiofréquences, tels que la téléphonie et l'Internet mobiles, les services de communication utilisés par les services de défense nationale et les forces de sécurité et de secours, les communications des pilotes d'avion, les alertes de détresse pour l'aviation et le maritime, la réception de données de synchronisation et de temps via le GPS ou Galileo (Galileo étant le GPS européen[202]), ainsi que des activités recourant à des communications ou à des échanges de données par voie hertzienne, tels que les services de transport, la météorologie, les objets connectés, l'industrie 4.0, les infrastructures connectées et les territoires intelligents.

Ces dernières années, le nombre de cas de brouillage et leur gravité sont en augmentation[203], en raison notamment, de l'évolution des technologies hertziennes (c'est-à-dire introduction de la 5G et de la 6G à venir en matière de téléphonie et d'Internet mobiles, technologies en mode partage de temps qui nécessitent une synchronisation très fine, utilisation de bandes de fréquences de plus en plus élevées, ..), de la densification des usages du spectre radioélectrique (introduction de nouveaux services dans des bandes de fréquences réservées (5G, 6G) ou dans des bandes de fréquences en partage avec d'autres services (WIFI 6) ; dépendance croissante, à la bonne réception du GPS, du fonctionnement d'activités et d'infrastructures ; développement des objets et capteurs connectés dans des entreprises ou des collectivités ; accroissement du nombre d'opérateurs de services satellitaires, etc.), de l'intensité de la présence d'équipements radioélectriques, électriques et électroniques, de la disponibilité en ligne de brouilleurs illicites et désormais aussi de l'usage d'IMSI-catchers illégaux utilisés pour intercepter le trafic de communications mobiles et de la dépendance

[202] Les systèmes GNSS de radionavigation par satellite apportent des informations en termes de positionnement et de temps. Plusieurs systèmes GNSS existent : le système américain GPS, le système européen Galileo, le système russe Glonass ou encore le système chinois Beidou.

[203] Sur les années 2021-2023, les agents de l'agence nationale des fréquences (ANFR) ont traité en moyenne un peu plus de 1600 infractions en matière de brouillage par an (contre 1212 en 2019). Ils ont également relevé (et fait corriger) en 2022 dans le cadre de contrôles préventifs, plus de 2100 non-conformités d'installations radioélectriques (23% des stations contrôlées présentaient au moins une anomalie) et plus de 2000 non-conformités de fréquences (téléphonie mobile exclue - 20% d'anomalie), c'est-à-dire plus 4 000 de infractions susceptibles d'être la cause de brouillages.

croissante de nombreuses activités à la disponibilité d'informations transmises sur des connexions sans fil.

Les brouillages peuvent être de nature volontaire ou causés par de la négligence.

Une des activités les plus préoccupantes est l'utilisation de brouilleurs pour lesquels la loi française[204] prévoit leur interdiction générale (importation, publicité, cession à titre gratuit ou onéreux, mise en circulation, installation, détention et utilisation).

Outre le fait qu'ils ne font de plus en plus partie de la panoplie des délinquants pour leurs méfaits, l'utilisation de brouilleurs peut avoir des conséquences graves pour la sécurité, notamment en raison de leurs effets collatéraux sur une zone beaucoup plus grande qu'imaginée (par exemple, un brouilleur de GPS utilisé par un employé qui veut empêcher la géolocalisation de son véhicule par son employeur peut perturber des avions volant à 2 000 mètres d'altitude ou stationnés à 500 mètres de sa position)[205]. Le brouillage du GPS ou de Galileo peut générer des situations à risques lors des phases d'approches à proximité des pistes, nécessitant une grande précision de géolocalisation, surtout en cas de mauvaises conditions météorologiques ou de relief accidenté.

Le leurrage du GNSS (« Global Navigation Satellite System » ou système de navigation par satellites tels que le GPS ou Galileo), qui consiste à envoyer de faux signaux sur les bandes GNSS pour tromper les récepteurs GNSS que ce soit en matière d'information de géolocalisation ou de temps, est une menace qui augmente du fait de la démocratisation des systèmes de radio logicielle (SDR) et de la disponibilité croissante sur le net de programmes informatiques ou de tutoriels dédiés. Or un leurrage du GNSS, plus insidieux qu'un brouillage, est une attaque très offensive avec des conséquences qui peuvent être très critiques notamment sur le transport aérien, maritime, fluvial et terrestre et les réseaux de communication.

Ainsi, les outils de guerre électronique, tels que les brouilleurs et les systèmes de leurrage ou de déception, sont d'ores et déjà présents sur notre territoire. Ils peuvent être utilisés par des

---

[204] Article L. 33-3-1 du CPCE : « I.- Sont prohibées l'une quelconque des activités suivantes : l'importation, la publicité, la cession à titre gratuit ou onéreux, la mise en circulation, l'installation, la détention et l'utilisation de tout dispositif destiné à rendre inopérants des équipements radioélectriques ou des appareils intégrant des équipements radioélectriques de tous types, tant pour l'émission que pour la réception. II.- Par dérogation au I du présent article et sans préjudice de l'article L. 213-2 du code de la sécurité intérieure, ces activités sont autorisées pour les besoins de l'ordre public, de la défense et de la sécurité nationale, ou du service public de la justice. »

[205] Autres exemples : un brouillage de grande ampleur du GPS affectait une grande partie du sud de la France en novembre 2019. Parmi les victimes, figuraient l'armée de l'air, les services de l'aviation civile et plusieurs aéroports du Sud de la France dont celui de Nice. Il était causé par un brouilleur GPS installé sur un yacht installé dans un port français. En mars 2021, un cas similaire causé par un brouilleur GPS à bord d'un yacht se trouvant dans un port hollandais a fait perdre le système AIS d'anticollision à tous les navires présents sur le fleuve l'Escaut. Il avait aussi empêché la réception du GPS par tous les avions volant dans le Nord de la France, la Belgique et les Pays-Bas.

individus particulièrement mal intentionnés, dont des terroristes, et leurs effets sont comparables à ce qui se passe sur des théâtres d'opération militaire.

Les brouillages, offensifs ou non intentionnels, présentent, dans le contexte « sans fil » des risques comparables à des menaces liées aux attaques informatiques. Un brouillage de fréquences génère en effet un « déni de service » des applications économiques, sociétales, sécuritaires et régaliennes qui utilisent ces fréquences pour la transmission ou la réception d'informations ou d'ordres sur des liaisons sans fil.

Les ministres chargés des Transports, de l'Intérieur et de l'Économie avaient saisi, en décembre 2017, le Conseil général de l'environnement, le Conseil général de l'économie et l'Inspection générale de l'administration qui ont formulé en octobre 2018 une série de recommandations[206] afin de faire évoluer le cadre juridique pour mieux lutter contre les perturbations préjudiciables du spectre de fréquences électromagnétiques et les brouilleurs illicites ce qui participe à la protection des citoyens, des entreprises et des services régaliens.

De plus, des travaux de réflexion menés en lien avec la Commission interministérielle de sûreté aérienne (CISA), la Commission interministérielle de coordination des réseaux et des services de communications électroniques (CICRESCE) et le Comité interministériel Galileo et son GT Lutte contre les Brouillages GNSS (GPS, Galileo) avaient permis d'aboutir à des propositions d'évolution des pouvoirs d'enquête des agents de ANFR ainsi que des sanctions pénales associées à ces brouillages.

Les propositions du rapport et des commissions mentionnées aux alinéas précédents relèvent la faiblesse de la sanction pénale associée au brouillage et aux brouilleurs.

En application du code des postes et des communications électroniques (CPCE), un brouillage est puni de six mois d'emprisonnement et 30 000 euros d'amende et l'utilisation d'un brouilleur est également punie de six mois d'emprisonnement et 30 000 euros d'amende. Or, à titre de comparaison, les sanctions en matière de cybersécurité dans le Code pénal sont beaucoup plus sévères que celles prévues par le CPCE[207].

Le niveau actuel des sanctions pénales (six mois de prison et 30 000 € d'amende) n'est pas cohérent avec le niveau des sanctions pour des attaques informatiques, alors qu'un brouillage porte atteinte à la disponibilité des informations véhiculées sur les liaisons hertziennes et que l'un des trois concepts fondamentaux en sécurité de l'information est la disponibilité. Par

[206] Rapport non disponible en ligne mais communicable sur demande.

[207] Article 323-2 du Code pénal : « le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de cinq ans d'emprisonnement et de 75000 € d'amende. Lorsque cette infraction a été commise à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine est portée à sept ans d'emprisonnement et à 100000 € d'amende ».

ailleurs, pour nombre d'applications et de secteurs, les enjeux liés à la disponibilité des systèmes priment sur la confidentialité ou l'authenticité.

Prévoir une sanction de trois ans d'emprisonnement minimum pour les brouillages est nécessaire pour disposer de pouvoirs d'enquête à la hauteur des enjeux, et ce, même si le temps de la flagrance est dépassé.

En effet, lors du traitement d'un brouillage ayant pour effet une atteinte grave à des services de sécurité et des services et infrastructures vitales de la nation, pour lequel l'ANFR sollicite le soutien d'un officier de police judiciaire (OPJ) pour finaliser sa recherche de la source de brouillage, si la période de flagrance est dépassée[208], il faut une peine d'un minimum de trois ans de prison pour qu'une perquisition ou une visite domiciliaire soit autorisée par le juge de la liberté et de la détention sans l'assentiment de la personne concernée et permette de faire cesser la perturbation[209].

Autre écueil en raison de la légèreté de la sanction actuelle, la perturbation des émissions hertziennes est peu poursuivie et peu sanctionnée (90 % des procès-verbaux transmis aux parquets sont classés sans suite). Le sentiment d'impunité qui en découle nuit tant à la prévention qu'à la prise de conscience par les auteurs de la nature délictuelle de l'acte et est susceptible d'entraîner des difficultés à faire cesser le délit, à empêcher les récidives et, ainsi, des perturbations du spectre graves et grandissantes. Le faible niveau actuel des sanctions pénales ne permet pas non plus une réponse judiciaire proportionnée pour des brouillages particulièrement offensifs ou qui ont de graves conséquences économiques, telles que le blocage d'un aéroport ou l'arrêt de fonctionnement d'une entreprise, ou dangereuses avec la mise en danger de la vie d'autrui, telle qu'un brouillage des fréquences de détresse maritime ou un brouillage du GPS de hélicoptères du SAMU.

Concernant les brouilleurs illicites, le niveau actuel faible de la sanction n'est pas assez dissuasif pour empêcher les achats de brouilleurs, notamment sur des sites Internet étrangers qui en font le commerce « illégal ».

1.2. CADRE CONSTITUTIONNEL

L'utilisation des fréquences radioélectriques sur le territoire de la République constitue un mode d'occupation privatif du domaine public de l'État[210]. Dans la décision du 26 juin 1986 relative aux lois de privatisation[211], le Conseil rappelle en ce sens que « les dispositions de la

[208] Dans le cadre, d'une enquête en flagrance, la perquisition sans assentiment de l'occupant des locaux est possible.

[209] Article 76 du code de procédure pénale.

[210] Voir en ce sens la décision n° 2000-442 DC du 28 décembre 2000 du Conseil constitutionnel.

[211] Décision n° 86-207 DC du 26 juin 1986.

Déclaration des droits de l'homme de 1789 relatives au droit de propriété et à la protection qui lui est due... ne concernent pas seulement la propriété privée des particuliers mais aussi, à un titre égal, la propriété de l'État et des autres personnes publiques ». Cette décision fonde le régime de police de conservation du domaine public dont les fréquences font partie en tant que domaine public hertzien.

Les sanctions prévues à l'article L. 39-1 du CPCE répondent au principe de légalité découlant de l'article 8 de la déclaration des droits de l'homme et du citoyen de 1789 qui dispose que « La loi ne doit établir que des peines strictement et évidemment nécessaires, et nul ne peut être puni qu'en vertu d'une loi établie et promulguée antérieurement au délit, et légalement appliquée ».

L'article 34 de la Constitution dispose que la loi fixe les règles concernant la détermination des crimes et délits ainsi que les peines qui leur sont applicables. La détermination des contraventions et des peines qui leur sont applicables ont, par voie de conséquence, un caractère réglementaire. Le domaine dévolu au pouvoir réglementaire n'est cependant pas sans limite. Il a été défini par le Conseil constitutionnel dans sa décision n° 73-80 L du 28 novembre 1973, lequel indique que la « détermination des contraventions et des peines qui leur sont applicables est du domaine réglementaire lorsque lesdites peines ne comportent pas de mesures privatives de liberté ».

En dehors du principe qui vient d'être exposé, l'article 8 de la Déclaration de 1789 emporte l'obligation pour le législateur de définir les incriminations en termes clairs et précis. La décision fondatrice est à cet égard la décision rendue les 19 et 20 janvier 1981[212] à propos de la loi dite « sécurité-liberté ».[213]

Le principe de nécessité des peines est un principe qui est affirmé par l'article 5 et également par l'article 8 de la Déclaration de 1789.

La disposition proposée prévoit un régime de sanctions proportionné aux infractions relevées et satisfait donc aux principes constitutionnels développés ci-avant.

1.3. CADRE CONVENTIONNEL

[212] Décision n° 80-127 DC du 20 janvier 1981.

[213] Le Conseil constitutionnel a énoncé à cette occasion (cons. 7) « qu'il (…) résulte (de l'article 8 de la Déclaration de 1789) la nécessité pour le législateur de définir les infractions en termes suffisamment clairs et précis pour exclure l'arbitraire ». Cette motivation a été souvent reprise depuis, et parfois complétée par l'indication que cette exigence résulte non seulement des dispositions de l'article 8 de la Déclaration, mais aussi de l'article 34 de la Constitution (n° 84-176 DC, 25 juillet 1984, cons. 6 ; n° 98-399, 5 mai 1998, cons. 7 ; n° 2001-455, 12 janvier 2002, cons. 82 ; n° 2004-492, 2 mars 2004, cons. 5).

Au niveau international, le droit en matière de bon fonctionnement des télécommunications est principalement régi par les travaux élaborés au sein de l'Union Internationale des Télécommunications (UIT), agence internationale de coopération technique de l'Organisation des Nations-Unies. Ce droit, largement fondé sur la coopération et la coordination entre États, découle de ses deux instruments fondamentaux : la Constitution de l'UIT et sa Convention établie en 1992 ayant valeur de traités internationaux. L'UIT produit des règlements administratifs considérés comme des instruments juridiques contraignants pour les États et faisant l'objet de révisions périodiques dans le cadre des conférences mondiales des radiocommunications (CMR) et des conférences régionales des radiocommunications (CRR).

Le règlement des radiocommunications (RR) adopté par ses membres sur le fondement d'une convention internationale, est l'un de ces règlements et il a force obligatoire pour lesdits membres. Les mesures portées s'inscrivent en conformité avec les obligations découlant de la participation de la France à l'UIT, notamment l'article 15 sur les brouillages du Règlement de Radiocommunications. Le point 15.12 du RR prévoit ainsi que «§ 8 Les administrations doivent prendre toutes les mesures pratiques nécessaires pour que le fonctionnement des appareils et installations électriques de toute espèce, y compris les réseaux de distribution d'énergie ou de télécommunication, mais à l'exception des appareils destinés aux utilisations industrielles, scientifiques et médicales, ne puisse pas causer de brouillage préjudiciable à un service de radiocommunication, et en particulier aux services de radionavigation et autres services de sécurité, exploité conformément au présent Règlement. »

En matière plus spécifiquement de sanction pour acte de brouillage, le point 15.20 du même RR rajoute « § 13 Si une administration a connaissance d'une infraction à la Constitution, à la Convention ou au Règlement des radiocommunications, (notamment à l'Article 45 de la Constitution et au numéro 15.1 du Règlement des radiocommunications), commise par une station relevant de sa juridiction, l'administration constate les faits et prend les mesures nécessaires. »

La prévention et la sanction des actes de brouillage s'imposent donc aux Etats parties à la convention de l'UIT, dont la France.

Le droit européen a établi, via la directive 2018/1972[214] un code européen des communications électroniques, transposé en droit français dans le CPCE. Cette mesure s'inscrit en conformité avec ces dispositions et en particulier celles de son article 29 relatif aux sanctions. Par ailleurs l'article 28 relatif à la coordination du spectre radioélectrique entre Etats membres prévoit que les Etats membres prennent toutes les mesures nécessaires à éviter un brouillage préjudiciable « sans préjudice des obligations qui leur incombent au titre du droit international et des accords internationaux applicables, tels que le règlement des

[214] Directive (UE) 2018/1972 du Parlement européen et du Conseil du 11 décembre 2018 établissant le code des communications électroniques européen.

radiocommunications de l'UIT ».
Ils sont à ce titre contraints de coopérer dans le cadre du RSPG (Radio Spectrum Policy Group) à la coordination transfrontière de l'utilisation du spectre radioélectrique.

L'obligation de prévenir le brouillage figure également à l'article 45 de la directive 2018/1972 « qu'il soit transfrontière ou national », « en prenant des mesures préventives et correctrices appropriées à cette fin ».

1.4. ÉLEMENTS DE DROIT COMPARE

Au **Royaume-Uni**, créer des interférences avec un brouilleur sur les bandes de télécommunications est un crime. La peine maximum pouvant être infligée est de deux ans d'emprisonnement assortie ou non d'une amende dont le montant ne serait pas plafonné : « *It is a crime to use any apparatus, including jammers, for the purposes of deliberately interfering with radio communications. The maximum penalty is 2 years imprisonment and/or an unlimited fine"*[215].

En **Espagne**, l'usage de tous les appareils qui perturbent les radiocommunications, créent des interférences, ou affectent l'usage des téléphones mobiles est soumis à autorisation du secrétariat d'État : l'utilisation de ce type d'appareils est réservée à la sécurité publique, à la défense nationale, à la sécurité de l'État et aux activités de l'État dans le cadre du droit pénal.

Les sanctions prévues vont d'une amende de 500 000 euros pour les infractions graves à 20 millions d'euros pour les infractions très graves.

En **Italie**, la législation italienne interdit l'usage de brouilleurs (sauf pour les forces de l'ordre) et prévoit des peines allant de un à cinq ans d'emprisonnement.

2. NECESSITE DE LEGIFERER ET OBJECTIFS POURSUIVIS

2.1. NECESSITE DE LEGIFERER

Protéger le spectre contre les brouillages et les brouilleurs illicites, c'est en conséquence protéger les activités et infrastructures (industries, services critiques, sécurité intérieure et défense nationale) qui permettent d'assurer la continuité de l'Etat et de la vie économique de la Nation.

[215] Section 68 of the Wireless Telegraphy Act 2006.

Le niveau actuel des sanctions pénales (six mois de prison et 30 000€ d'amende) n'est pas adapté à la diversité des cas de brouillage.

En raison de leur caractère volontairement offensif et de leurs conséquences potentiellement dangereuses, les activités illicites impliquant des brouilleurs justifient des sanctions encore accrues : cinq ans d'emprisonnement et 150 000 euros d'amende.

Il en est de même pour les utilisations illégales de fréquences attribuées par le Premier ministre en application de l'article L. 41-1 du CPCE pour les besoins de la défense nationale et de la sécurité publique, ou d'installations radioélectriques utilisant ces mêmes fréquences du fait de la menace potentielle posée aux intérêts fondamentaux de la nation. Le quantum des peines, actuellement fixé à six mois de prison et 30 000 euros d'amende, resterait inchangé pour tous les autres cas d'utilisation illégale d'une fréquence (donc hors besoins de la défense nationale et sécurité publique).

Ce souhait est né du constat de plusieurs cas d'utilisation des fréquences de la défense nationale sans demande d'autorisation pour des objectifs qui apparaissaient suspects.

Par ailleurs, le risque de leurrage du GPS inquiète fortement l'aviation civile (émission de signaux trompeurs sur les fréquences GPS et Galileo attribuées au ministère des armées). Sans l'évolution proposée, la sanction maximum pour leurrage resterait à six mois de prison et 30 000 euros d'amende alors qu'il s'agit d'une attaque fréquentielle extrêmement critique.

Enfin, il apparaît que de nombreuses stations radioélectriques ne respectent pas les caractéristiques qu'elles ont déclarées en vue d'obtenir l'accord d'implantation délivré par l'ANFR, en application du I de l'article L. 43. Actuellement, seule l'absence d'accord est sanctionnée. Or, une puissance ou une orientation d'antenne différentes de celles autorisées peuvent être source de brouillage.

Disposer de sanctions pénales renforcées comme exprimées ci-dessus pour des cas de non-conformité, des cas de brouillages, des infractions liées à des brouilleurs ou relatives à des fréquences attribuées par le Premier ministre pour les besoins de la défense nationale et de la sécurité publique, implique de modifier l'article L. 39-1 du CPCE qui se trouve dans la partie législative de ce code, et pour ce faire, nécessite un vecteur législatif qui est la loi dite « résilience ».

La mesure comportant des dispositions relatives à la privation de liberté, elle relève nécessairement du niveau législatif.

2.2. OBJECTIFS POURSUIVIS

L'objectif poursuivi en faisant évoluer les dispositions actuelles du CPCE est d'avoir des sanctions pénales graduées avec des quantums de peines plus élevés afin de disposer d'une

dissuasion plus efficace, ceci afin de maintenir les capacités de sécurité intérieure et de défense nationale et protéger des attaques du spectre radioélectrique tant les services, entreprises et infrastructures d'importance vitale que les citoyens.

3. OPTIONS POSSIBLES ET DISPOSITIF RETENU

3.1. OPTIONS ENVISAGEES

Aucune autre option n'a été envisagée.

3.2. OPTION RETENUE

Le projet de texte vise à modifier l'article L. 39-1 du CPCE afin d'adapter le cadre législatif relatif à la lutte contre les perturbations du spectre et les bouilleurs illicites.

3.2.1. Nouvelle gradation dans le quantum des peines

Il est proposé de conserver le libellé des infractions pénales mentionnées à l'article L. 39-1 du CPCE.

En revanche, il est prévu une augmentation et adaptation 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 ;
    - 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 ;

– 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 (pour les seules fréquences attribuées par le Premier ministre en application de l'article L. 41 du CPCE pour les besoins de la défense nationale et de la sécurité publique) ;

3.2.2. Création d'une nouvelle infraction

Une nouvelle infraction est créée 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, préalable à son implantation.

4. ANALYSE DES IMPACTS DES DISPOSITIONS ENVISAGEES

4.1. IMPACTS JURIDIQUES

4.1.1. Impacts sur l'ordre juridique interne

Les présentes dispositions modifient l'article L. 39-1 du CPCE.

4.1.2. Articulation avec le droit international et le droit de l'Union européenne

Hormis un cas particulier qui n'est pas concerné par les dispositions de l'article 41 du projet de loi[216], la directive (UE) 2018/972 précitée laisse une grande latitude aux Etats membres pour prévoir un régime de sanctions approprié. Les Etats membres doivent simplement respecter l'obligation de prévoir des sanctions appropriées, effectives, proportionnées et dissuasives.

4.2. IMPACTS ECONOMIQUES ET FINANCIERS

4.2.1. Impacts macroéconomiques

Pas d'impact attendu.

4.2.2. Impacts sur les entreprises

[216] Il s'agit du non-respect des dispositions relatives au relevé géographique figurant à l'article 22 de la directive (UE) 2018/1972.

Les impacts sur les entreprises sont difficiles à quantifier.

Même si leur nombre devrait évoluer à la hausse, le nombre d'entreprises effectivement condamnées pour avoir commis un délit pour non-respect des dispositions sur le spectre radioélectrique ne devrait pas dépasser une centaine par an.

Dans la plupart des cas, la hausse des quantums aura un effet positif sur le délais mis en œuvre par l'entreprise concernée pour faire cesser l'infraction. A titre d'exemple, un opérateur de réseau de communications électroniques mettra plus rapidement la station radioélectrique qu'il exploite en conformité avec les caractéristiques sur lesquelles est basée l'autorisation dont il bénéficie que ce qu'il peut être constaté actuellement.

En revanche, une amélioration de la lutte contre les brouillages protègera entreprise et collectivités car elle permettra de diminuer la menace d'un brouillage et le risque associé qui peut être l'arrêt de son activité tant que le brouillage n'est pas résolu.

C'est le cas, par exemple, de toutes celles qui utilisent les signaux GNSS pour bénéficier de la géolocalisation ou de la synchronisation, parfois actuellement interrompus par des brouillages intempestifs. Une antenne 4G ou 5G TDD d'un réseau d'opérateur mobile public ou privé ne peut fonctionner correctement sans une bonne synchronisation. Celle-ci est délivrée par le GPS. Un brouillage du GPS peut aboutir à la perte de l'utilisation de l'antenne relais correspondante.

C'est également le cas des entreprises qui utilisent des réseaux pour la communication mobile de leurs salariés, la connexion de capteurs, de machines-outils, de machines de transport, de services de logistique, d'équipements de vidéoprotection, etc.

C'est le cas d'infrastructures dont le fonctionnement, la maintenance et /ou la sécurité reposent sur l'échange de données sur des réseaux sans fil.

Enfin, les collectivités menant des projets de territoires intelligents, tels que des réseaux de capteurs qui détectent des risques de crue ou des départs de feux ou qui permettent de suivre le trajet des bus municipaux et remontent leurs informations à la mairie et aux services de secours via des liaisons sans fil (technologies LORA, WIFI, 4G ou 5G verticales, réseaux professionnels privés, Faisceaux Hertziens, ou autre, etc.).

4.2.3. Impacts budgétaires

Pas d'impact attendu.

4.3. IMPACTS SUR LES COLLECTIVITES TERRITORIALES

Les collectivités territoriales pourront bénéficier d'un spectre radioélectrique moins brouillé que ce soit pour les communications électroniques de leurs administrés pour des activités personnelles et professionnelles, les communications électroniques des services de sécurité et de secours et tous autres services que la collectivité met en place et qui utilisent de la connectivité sans fil (territoires intelligents).

Par ailleurs, en tant qu'utilisatrices d'équipements radioélectriques qui seraient utilisés de manière non conforme et causeraient un brouillage, elles seraient incitées à se mettre plus rapidement en conformité afin de faire cesser certaines infractions. C'est le cas par exemple des réseaux WIFI que certaines communes installent pour connecter des systèmes de vidéoprotection ou fournir un service WIFI dans des espaces publics extérieurs, qui doivent respecter les dispositions réglementaires de l'ARCEP afin de ne pas brouiller les radars de la météorologie et altérer ou empêcher les prévisions en matière de précipitations et d'orage de Météo France.

L'effet plus dissuasif des sanctions en cas de brouillage aurait aussi un effet préventif en encourageant les installateurs et les revendeurs d'équipements radioélectriques à suivre le cadre réglementaire afin de limiter les risques de brouillage.

4.4. IMPACTS SUR LES SERVICES ADMINISTRATIFS

Ces dispositions ne sont pas de nature à créer des charges nouvelles pour les services administratifs de l'Etat et plus particulièrement au sein de l'Agence nationale des fréquences – Aucune création d'emplois publics ne sera nécessaire.

4.5. IMPACTS SOCIAUX

Pas d'impact attendu.

4.5.1. Impacts sur la société

Les présentes dispositions, en protégeant mieux le spectre des attaques, contribueront à maintenir les capacités de sécurité intérieure et de défense nationale et à protéger les services, entreprises et infrastructures d'importance vitale et les citoyens. Le brouillage d'une bande de fréquences peut engendrer des conséquences graves et dangereuses, y compris la mise en danger d'autrui, notamment s'il affecte la disponibilité de réseaux dédiés à la défense nationale ou la sécurité publique. Les dispositions permettent en effet de protéger la continuité des réseaux sans fil utilisés par les forces de sécurité et de secours (policiers nationaux et municipaux, gendarmes, pompiers, SAMU, préfets, douaniers, forces armées, agents du ministère de la Justice ainsi que certains opérateurs dits « d'importance vitale »). Les

précédentes dispositions permettent aussi de protéger la continuité de collectivités, d'infrastructures et d'entreprises utilisant des réseaux sans fil.

4.5.2. Impacts sur les personnes en situation de handicap

Sans objet.

4.5.3. Impacts sur l'égalité entre les femmes et les hommes

Sans objet.

4.5.4. Impacts sur la jeunesse

Sans objet.

4.5.5. Impacts sur les professions réglementées

Sans objet.

4.6. IMPACTS SUR LES PARTICULIERS

Les précédentes dispositions auront un impact positif sur la protection des particuliers en permettant la continuité des services qui leur sont essentiels et qui utilisent des liaisons hertziennes : les communications téléphoniques sur leur portable, les envois de mail et la consultation de l'Internet sur leur portable, la possibilité de faire un appel d'urgence, les appels dans les ascenseurs en cas de panne ; la réception des alertes FR Alert pour qu'ils puissent prendre des mesures pour se protéger le cas échéant, les services de géolocalisation dans leur voiture ou leur téléphone, le babyphone installé dans la chambre d'enfants, des prévisions météorologiques fiables, des services de transport sûrs, voitures connectées, le réseau de sécurité des trains, etc.

4.7. IMPACTS ENVIRONNEMENTAUX

La meilleure protection du spectre contre les brouillages bénéficie à toutes sortes d'applications utilisant des liaisons sans fil, dont des applications visant à renforcer la protection environnementale (réseau de capteurs connectés par un réseau sans fil).

Inversement, certains brouillages peuvent contribuer à l'augmentation de risques environnementaux.

Par exemple, en matière de transport maritime, fluvial et d'opérations portuaires, le brouillage du GNSS peut avoir des impacts en termes de sécurité des personnes (atteinte à la vie humaine), de sécurité des biens (navires endommagés, marchandises dégradées ou perdues, etc.), de répercussions négatives au plan économique (coûts supplémentaires engendrés par retards de livraison, navigation moins optimisée, incapacité à mener des opérations de surveillance par drones, etc.).mais également en matière d'environnement (pollutions, surconsommation de carburant etc.) [217].

5. CONSULTATIONS ET MODALITES D'APPLICATION

5.1. CONSULTATIONS MENEES

En application de l'article L. 1212-2 du code général des collectivités territoriales, le présent article a été soumis à l'examen du Conseil national d'évaluation des normes (CNEN), qui a rendu un avis défavorable, le 22 mai 2024.

En application de l'article L. 36-5 du code des postes et des communications électroniques, l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse (ARCEP) a été saisie pour avis le 7 mai 2024 sur l'ensemble du projet de loi. Cette dernière a rendu un avis favorable le 23 mai 2024 en ce sens qu'il ne comprend aucune remarque concernant le présent article.

Sur le fondement de l'article 8 de la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, la Commission nationale de l'informatique et des libertés (CNIL) a été consultée à titre facultatif.

5.2. MODALITES D'APPLICATION

5.2.1. Application dans le temps

Les nouvelles dispositions entreront en vigueur le lendemain de la publication de la loi au *Journal officiel* de la République française.

5.2.2. Application dans l'espace

Les nouvelles dispositions s'appliquent en Métropole.

[217] Cf. Guide de sensibilisation des acteurs du transport maritime & fluvial, édité en février 2024 par la DGITM et l'ANFR : guide non disponible en ligne mais communicable sur demande.

L’article est applicable de plein droit dans les départements relevant de l’article 73 de la Constitution (Guadeloupe, Guyane, Martinique, Mayotte, La Réunion).

Il est applicable à Saint Barthélémy, Saint-Pierre et Miquelon et Saint Martin sans qu’il y’ait lieu de prévoir de mention particulière d’applicabilité.

Les compétences de la collectivité de Saint-Barthélemy, énumérées à l’article LO 6214-3 du code général des collectivités territoriales, ne portent pas sur les sujets relevant du code des postes et communications électroniques

Les compétences de la collectivité de Saint-Martin, énumérées à l’article LO 6314-3 du code général des collectivités territoriales, ne portent pas sur les sujets relevant du code des postes et communications électroniques.

Les compétences de la collectivité de Saint-Pierre-et-Miquelon, énumérées à l’article LO 6414-1 du code général des collectivités territoriales, ne portent pas sur les sujets relevant du code des postes et communications électroniques.

5.2.3. Textes d’application

Les présentes dispositions ne requièrent aucune mesure d’application.

Article 42 – Renforcement des conditions d'accès à une assignation de fréquences déposées par la France auprès de l'Union Internationale des Télécommunications

1. ÉTAT DES LIEUX

1.1. CADRE GENERAL

Afin de délivrer un service, les systèmes satellitaires orbitaux[218] 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 commandé 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 (ensemble dénommé « filing ») 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'Union Internationale des Télécommunications (UIT), agence de l'ONU spécialisées dans les technologies de l'information et de la communication met en œuvre un processus - préalable à tout lancement de satellites - de déclaration des fréquences associées. Le Règlement des radiocommunications (RR), révisé par les États membres à chaque Conférence mondiale des radiocommunications, décrit précisément les procédures, y compris la coordination entre Etats membres, visant à assurer la disponibilité des fréquences et l'absence de brouillage.

En pratique, il revient aux États de déposer auprès de l'Union Internationale des Télécommunications (UIT) une demande d'enregistrement portant à la fois sur une ou plusieurs bandes de fréquences et sur une position orbitale donnée. En cas de problématique de coexistence, l'utilisateur de la demande d'enregistrement la plus ancienne est prioritaire vis-à-vis des autres utilisateurs, ces derniers devant adapter leurs émissions radioélectriques pour ne pas perturber l'activité du premier.

Conformément au code des postes et des télécommunications, et notamment de son article L. 43, 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*

[218] Ensemble de satellites artificiels mis en orbite dans l'espace extra atmosphérique.

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.

Pour les demandeurs, le processus est le suivant :

- Les opérateurs souhaitant exploiter un système à satellites commencent par déposer une demande de coordination auprès de l'administration compétente d'un État membre de l'UIT (l'ANFr en France[219]), qui la dépose ensuite auprès de l'UIT. En France, le code des postes et communications électroniques (CPCE) limite les motifs de refus de déclaration auprès de l'UIT à la conformité au tableau national de répartition des bandes de fréquences et aux stipulations des instruments de l'UIT (I de l'article L. 97-2) ;
- L'étape suivante de la procédure prévue par le RR est la coordination avec tous les pays identifiés comme pouvant être affectés par le système proposé et le pays qui propose ce système. Cette coordination formelle prend la forme de négociations entre les administrations concernées des États membres de l'UIT affectés, en pratique relayées par les discussions entre les opérateurs concernés. À l'issue des négociations, l'administration notifie auprès de l'UIT le système à satellites, avec les caractéristiques finales du projet de l'opérateur qui l'a sollicité (bande de fréquences, orbite, zone de service) ;
- Après examen par les services de l'UIT, les assignations de fréquences et les orbites demandées sont définitivement inscrites dans le MIFR (*Master International Frequency Register*). L'enregistrement des fréquences et des orbites concernées dans le MIFR vaut reconnaissance internationale du réseau considéré, qui bénéficiera à partir de ce moment d'une antériorité, liée à la date du dépôt initial, lui garantissant une priorisation en matière de protection vis-à-vis des brouillages sur les projets de systèmes satellitaires ultérieurs ;
- L'opérateur satellitaire doit enfin obtenir une autorisation nationale dans le pays qui a négocié la coordination en son nom, pour exploiter ces assignations de fréquences spatiales. En France, il devra pour cela déposer un nouveau dossier auprès de l'ANFr. À l'issue de l'instruction du dossier et après avoir consulté les différentes parties prenantes (administrations affectataires et autres opérateurs potentiellement concernés), l'agence émettra un avis auprès du ministre en charge des communications électroniques, qui pourra prendre le cas échéant un arrêté ministériel d'autorisation.

La procédure relevant du niveau national est décrite à l'article L. 97-2 du CPCE.

[219] L'article L. 43 du CPCE prévoit que l'ANFr « prépare la position française et coordonne l'action de la représentation française dans les négociations internationales dans le domaine des fréquences radioélectriques »

L'ANFr se charge également, en lien avec l'utilisateur de l'enregistrement, des différentes formalités à accomplir au nom de la France auprès de l'UIT pour assurer la gestion de ces assignations et notamment de la conduite des négociations avec les autres usagers d'enregistrement auprès de l'UIT (que ces enregistrements aient été déclarés par la France ou non).

En l'état actuel du droit interne, une demande d'exploitation d'une assignation de fréquence à un système satellitaire, déclarée par la France à l'Union internationale des télécommunications, peut quant à elle être refusée pour les raisons suivantes (2. du I. de l'article L. 92-2 du CPCE) :

1. Pour la sauvegarde de l'ordre public, les besoins de la défense ou ceux de la sécurité publique ;
2. 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 ;
3. Lorsque la demande a des incidences sur les droits attachés aux assignations de fréquence antérieurement déclarées par la France à l'Union internationale des télécommunications ;
4. Lorsque le demandeur a fait l'objet d'une des sanctions prévues au III du présent article 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 mette 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. La procédure prévue aux 2° et 5° de l'article L. 36-11 est applicable. Il peut, en outre, décider d'interrompre la procédure engagée par la France auprès de l'Union internationale des télécommunications.

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'Union internationale des télécommunications, 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.

En 2023, l'ANFr a traité 55 demandes de dépôts d'assignations[220]. Elle estime que de l'ordre de trois cas par an seraient susceptibles de faire l'objet d'un contrôle approfondi au titre des nouvelles dispositions.

De même, selon les estimations de l'agence, cette dernière reçoit trois à quatre demandes d'autorisation d'exploitation d'assignation par année. Le nombre de cas susceptibles de faire l'objet d'un contrôle approfondi au titre des nouvelles dispositions sera donc en pratique extrêmement limité.

Enfin, on peut noter qu'en l'état actuel du droit, le refus d'autoriser un acteur à exploiter une assignation déposée par la France auprès de l'UIT est un évènement très rare (moins d'un par an). Si les dispositions proposées visent à renforcer les conditions afférentes à l'obtention d'une autorisation d'exploitation une assignation déposées par la France auprès de l'UIT, le nombre de refus ne devrait pas évoluer significativement (les acteurs seront informés en amont du dépôt de leur dossier de l'évolution du cadre légal et réglementaire, il est probable que ceux susceptibles de se voir opposer un refus renoncent à candidater).

1.2. CADRE CONSTITUTIONNEL

L'utilisation des fréquences radioélectriques sur le territoire de la République constitue un mode d'occupation privatif du domaine public de l'État[221]. Dans la décision du 26 juin 1986 relative aux lois de privatisation[222], le Conseil constitutionnel rappelle en ce sens que « les dispositions de la Déclaration des droits de l'homme de 1789 relatives au droit de propriété et à la protection qui lui est due [...] ne concernent pas seulement la propriété privée des particuliers mais aussi, à un titre égal, la propriété de l'État et des autres personnes publiques ». Cette décision fonde le régime de police de conservation du domaine public dont les fréquences font partie en tant que domaine public hertzien. Dès lors, les fréquences sont soumises à un dispositif d'autorisation préalable.

Les mesures envisagées devront également respecter le principe de liberté de commerce et de l'industrie fondée sur les articles 4 et 17 de la Déclaration des Droits de l'Homme et du Citoyen de 1789 ainsi que la liberté d'entreprendre reconnue comme principe à valeur constitutionnelle[223]. Ces libertés garantissent à tout individu le droit d'exercer librement une activité économique et ce dans le cadre du libre jeu de la concurrence. En outre, le respect de la liberté du commerce et de l'industrie implique que les personnes publiques n'imposent pas

[220] L'ANFR estime que la moyenne annuelle de demande traitée est de 60 par an.

[221] Voir en ce sens la décision n° 2000-442 DC du 28 décembre 2000 du Conseil constitutionnel.

[222] Décision n° 86-207 DC du 26 juin 1986.

[223] CC, 16 janvier 1982, n°81-132 DC.

de restrictions injustifiées et disproportionnées au regard de l'objectif poursuivi[224]. Dès lors, toute condition ou restriction imposée pour la délivrance des autorisations d'utilisation de fréquences ne devront pas porter atteinte de manière disproportionnée à ces libertés et poursuivre un objectif d'intérêt général. En l'espèce, la mesure proposée vise à assurer le respect des engagements internationaux de la France, l'existence d'un lien économique et la sécurité nationale. Le Conseil constitutionnel a d'ailleurs admis qu'il était possible de soumettre à autorisation des équipements radioélectriques afin de préserver les intérêts fondamentaux de la nation dont fait partie la sécurité nationale[225].

1.3. CADRE CONVENTIONNEL

Au niveau international, le droit en matière de bon fonctionnement des télécommunications est principalement régi par les travaux élaborés au sein de l'Union Internationale des Télécommunications (UIT), agence internationale de coopération technique de l'Organisation des Nations-Unies. Ce droit, largement fondé sur la coopération et la coordination entre États, découle de ses deux instruments fondamentaux : la Constitution de l'UIT et sa Convention établie en 1992 ayant valeur de traités internationaux. L'UIT produit des règlements administratifs considérés comme des instruments juridiques contraignants[226] pour les États et faisant l'objet de révisions périodiques dans le cadre des conférences mondiales des radiocommunications (CMR) et des conférences régionales des radiocommunications (CRR).

Le règlement des radiocommunications (RR) adopté par ses membres sur le fondement d'une convention internationale, est l'un de ces règlements et il a force obligatoire pour lesdits membres. En particulier, il fixe des normes générales que doit respecter tout système satellitaire et définit une procédure de « coordination internationale » à laquelle toute mise en orbite est subordonnée. Elle consiste, pour l'opérateur souhaitant exploiter un système satellitaire, à s'adresser à l'autorité compétente d'un État membre de l'UIT[227] pour que celle-ci dépose une demande d'inscription au fichier de référence international des fréquences. Cela permet aux autorités des autres Etats de prendre connaissance du projet et de réclamer la prise en compte d'éventuels risques de collision ou de brouillage avec des systèmes déjà inscrits ou en voie de l'être. Il revient ensuite à l'opérateur d'obtenir de l'État ayant déposé la demande d'enregistrement une autorisation d'exploitation de l'assignation associée. Cette autorisation fixe les caractéristiques d'orbite, de fréquences de communication ainsi que toute prescription à respecter pour se conformer aux normes du règlement des radiocommunications et tenir compte de la coordination internationale.

---

[224] Conseil constitutionnel, décision n° 2000-429 DC, 30 mai 2000.

[225] CC, 5 février 2021, n°2020-882 QPC.

[226] Article 54 de la Constitution de l'UIT.

[227] L'ANFr en France.

En France, l'ANFr est l'administration en charge de mettre en œuvre le processus auprès de l'UIT, l'autorisation d'exploiter relevant du ministre en charge des communications électroniques. Elle s'assure à ce titre de la conformité de la demande d'assignation qui lui est adressée aux dispositions du RR puis engage la procédure prévue à ses articles 9 (soumission et coordination des assignations) et 11 (notification des assignations). Cette activité correspond au I de l'article L. 97-2 du CPCE.

L'obtention de l'autorisation d'exploitation des assignations est quant à elle régie par le II de l'article L. 97-2 du CPCE.

A ce titre, on notera que le RR ne traite que de l'assignation de fréquences à des « administrations », entendus comme les États partis au traité :

Point 8.1 de l'article 8 du traité : « Au niveau international, les droits et les obligations des administrations vis-à-vis de leurs propres assignations de fréquence et de celles des autres administrations dépendent de l'inscription desdites assignations dans le Fichier de référence international des fréquences (Fichier de référence) ou de leur conformité, selon le cas, avec un plan. Ces droits sont assujettis aux dispositions du Règlement et aux dispositions de tout plan d'assignation ou d'allotissement de fréquence correspondant. »

En particulier, aucune disposition du RR ne précise dans quelles conditions les États peuvent autoriser des acteurs privés à exploiter des assignations déposées auprès de l'UIT, ces premiers demeurent donc libres d'y attacher toutes conditions qu'ils jugent nécessaires, étant entendu qu'ils sont tenus responsables auprès de l'UIT des brouillages potentiels que pourraient occasionner ces acteurs dans le cadre de l'exploitation desdites assignations, conformément aux points 15.33 à 15.46 de l'article 15 du traité. Les dispositions portées par le projet de modification de l'article L. 97-2 du code des postes et des communications électroniques participent en conséquence au respect par la France de ses engagements internationaux.

1.4. ÉLEMENTS DE DROIT COMPARE

Dans le cas du Royaume-Uni, les missions de déclaration des assignations et de leur autorisation d'utilisation sont confiées à l'OFCOM (*Office of Communications*) qui a aussi le rôle de régulateur des stations terriennes communiquant avec des satellites sur leur territoire. En France, l'ANFr traite les assignations à des systèmes spatiaux, les trois régulateurs civils, à savoir l'ARCEP en métropole et dans les DROM, la Direction générale de l'économie numérique (DGEN) pour le gouvernement de Polynésie et l'Office des postes et des télécommunications (OPT) pour le gouvernement de Nouvelle-Calédonie autorisent les stations terriennes sur leurs territoires de compétence.

Si les procédures de traitement des demandes d'assignations à des systèmes spatiaux vis-à-vis de l'UIT sont identiques, les procédures nationales d'autorisation de l'exploitation diffèrent. Les missions de l'OFCOM découlent du texte « *The Wireless Telegraphy Act 2006* » et les principales différences en matière d'assignations et d'autorisations à des systèmes spatiaux sont listées ci-après :

- Les demandes d'assignations ne peuvent être faites que par des sociétés privées immatriculées en Grande-Bretagne ;
- Les demandes d'autorisation d'exploitation des assignations ne peuvent être faites que par des sociétés immatriculées en Grande-Bretagne ;
- L'OFCOM ne publie pas d'autorisation avec des conditions particulières par demandeur mais édicte des règles qui doivent être suives par tous les utilisateurs de fréquences spatiales britanniques.

Dans le cas des États-Unis d'Amérique, les missions de déclaration des assignations spatiales et de leur autorisation d'utilisation sont confiées à la FCC suivant le « Communications Act of 1934 ». La FCC est également le régulateur unique des stations terriennes communiquant avec des satellites depuis leur territoire.

Les procédures de traitement des assignations préalablement à l'envoi à l'UIT et les procédures d'autorisation de l'exploitation diffèrent. Par rapport au cadre français, les principales différences en matière d'assignations et d'autorisations à des systèmes spatiaux sont listées ci-après :

- Les demandes d'assignations ne peuvent être faites que par des sociétés privées immatriculées aux Etats-Unis ;
- Les conditions préalables à la déclaration des demandes assignations portent comme en France sur le respect de leur tableau national des fréquences et le respect du RR, mais elles sont complétées par l'obligation de respecter les contraintes de leur loi spatiale et d'effectuer une coordination préalable avec les autres utilisateurs gouvernementaux américains. La contrainte du respect de la loi spatiale américaine est plus forte que celle qu'impliquent les modifications proposées par les écritures objets de cette fiche, car elle sous-entend une accréditation du satellite concerné par la FCC (Federal Communications Commission) ;
- C'est la FCC qui publie des autorisations d'exploitation des assignations à des systèmes spatiaux.

Concernant les pays de l'Union européenne, les situations sont diverses :

- En règle générale, les demandes d'assignations ne peuvent être faites que par des sociétés enregistrées dans le pays (cas de la Croatie[228], des Pays-Bas et de la Norvège[229]). Certains Etats, comme les Pays-Bas, exigent également la description des activités économiques actuelles ou envisagées dans le pays, ainsi que l'installation d'un moyen de contrôle des émissions du satellite sur son territoire (une antenne ou un centre de contrôle), tandis que d'autres, comme la Suède, imposent que la demande soit produite par un ressortissant national ;
- De même, les demandes d'autorisation d'exploitation d'assignations de fréquences déposées par les États auprès de l'UIT sont généralement conditionnées à l'enregistrement des sociétés sur le territoire national ;
- En matière de procédure, si certains États n'exigent de la part des demandeurs d'autorisation d'exploitation d'assignation que le respect d'un ensemble de conditions comme en Grande Bretagne, la majorité des législations exige une autorisation individuelle explicite des demandeurs (cas de l'Allemagne[230]), ou la conclusion d'une convention entre le régulateur national et chaque demandeur d'autorisation (cas des Pays-Bas) ;
- Certains pays sont plus exigeants que les autorités françaises. A titre d'exemple, les autorités allemandes exigent que les satellites ayant vocation à exploiter une assignation déposée auprès de l'UIT soient désorbités une fois la fin de leur durée de vie atteinte.

2. NECESSITE DE LEGIFERER ET OBJECTIFS POURSUIVIS

2.1. NECESSITE DE LEGIFERER

Alors que de nombreux acteurs souhaitent déployer des constellations en orbite basse, la possibilité d'exploiter des bandes de fréquences sans risque de brouillage constitue un enjeu crucial car il conditionne le bon fonctionnement du service. À ce titre, le choix de l'État à solliciter afin de bénéficier d'une autorisation d'exploitation d'assignation déposée auprès de l'UIT est structurant : son administration sera en charge de défendre les droits de l'acteur concernant l'assignation déposée auprès de l'UIT vis à vis des autres utilisateurs du spectre au sein de l'UIT, afin notamment d'éviter les risques de brouillage.

---

228 http://www.porezna-uprava.hr/en/Pages/PIN.aspx.

229 https://nkom.no/english/satellite/satellite-registration/_/attachment/download/d8f9130c-c0c5-4cf1-939e-4dc9e17c9afd:ef979521aee54d4130ce1d24414d22c967dae64b/Regulations%20on%20coordination%20and%20use%20of%20satellite%20filings%20in%20Norway%20(unofficial%20translation).pdf.

230 https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Frequenzen/SpezielleAnwendungen/Satellitenfunk/VVSatSys_EN.pdf

La France dispose dans ce cadre d'une position singulière : l'Agence Nationale des Fréquences (ANFr), qui est en charge d'agir au nom de la France auprès de l'UIT, y dispose d'une reconnaissance importante en raison de son implication forte dans les travaux de l'organisation. L'ANFr est particulièrement reconnue pour le sérieux des analyses techniques qu'elle produit, notamment en ce qui concerne les conditions de coexistence entre systèmes satellitaires.

En conséquence, de nombreux acteurs internationaux font le choix de s'adresser à la France afin de bénéficier d'une autorisation d'exploiter une assignation de fréquence déposée auprès de l'UIT. Si cette situation est souhaitable et doit perdurer, il parait nécessaire de s'assurer que les acteurs privés qui bénéficient de l'expertise française en matière de gestion des fréquences ne nuisent pas aux intérêts de la sécurité et de la défense nationale et puissent, en retour à l'accompagnement qui leur est offert, apporter un bénéfice à l'économie française. D'autre part, la France dispose en effet d'un patrimoine exceptionnel en la matière (le 3ème plus important au niveau mondial) en particulier dans les bandes de fréquences Ku, Ka et Qv. Néanmoins, l'état du droit actuel ne permet pas de valoriser efficacement ce patrimoine : la marge de manœuvre de l'État quant à la décision d'autoriser ou non un acteur à utiliser ces ressources est particulièrement réduite.

C'est l'objet du projet de modification de la partie législative du code des postes et des communications électroniques, et notamment de l'article L. 97-2 dudit code, portée par ce projet de loi qui vise à étendre la marge de manœuvre de l'État avant, durant et après le processus d'autorisation.

2.2. OBJECTIFS POURSUIVIS

L'objectif de la mesure est :

- de conditionner le dépôt par l'ANFr d'une demande d'enregistrement auprès de l'UIT suite à une demande d'un acteur privé à l'existence d'un intérêt économique justifiant que la déclaration soit effectuée au nom de la France et le fait que les assignations en question ne soient pas de nature à compromettre les intérêts de la sécurité nationale et le respect par la France de ses engagements internationaux ;
- de conditionner l'attribution d'une autorisation d'exploiter une assignation déposée auprès de l'UIT à un acteur privé à ce que :
    - L'exploitation de cette attribution ne contrevienne ni aux besoins de la défense nationale ni au respect par la France de ses engagements internationaux ;
    - 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 durablement face aux obligations résultant de l'obtention de l'autorisation.

– d’assortir, le cas échéant, l’autorisation de conditions visant à assurer que les activités prévues dans le cadre de l’exploitation de l’assignation autorisée ne porteront pas atteinte aux intérêts de la sécurité et de la défense nationale ou le respect par la France de ses engagements internationaux ;

– de préciser les sanctions auxquelles s’expose le titulaire d’une autorisation d’exploitation d’une assignation déposée auprès de l’UIT, dans l’hypothèse où il ne respecterait pas les obligations qui lui sont imposées par les textes législatifs ou réglementaires.

3. OPTIONS POSSIBLES ET DISPOSITIF RETENU

3.1. OPTIONS ENVISAGEES

Aucune autre option n’a été envisagée.

3.2. OPTION RETENUE

Le présent article :

– complète le 1. du I. de l’article L. 97-2 du CPCE afin de préciser les conditions dans lesquelles un acteur privé peut demander à ce que l’ANFr dépose auprès de l’UIT une demande d’assignation. Ces conditions concernent notamment l’existence d’un intérêt économique justifiant que la déclaration soit effectuée au nom de la France et le fait que les assignations en question ne soient pas de nature à compromettre les intérêts de la sécurité nationale et le respect par la France de ses engagements internationaux ;

– complète le 2. du I. de l’article L. 97-2 afin de préciser les conditions dans lesquelles un acteur privé peut bénéficier d’une autorisation d’exploitation d’une assignation déposée par la France auprès de l’UIT. Il s’agit en particulier d’assurer que cette autorisation soit accordée à une entité de droit français ou à un établissement immatriculé au registre du commerce et des sociétés en France, que l’attribution de cette autorisation ne soit pas opposée 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. Le cas échéant, l’autorisation peut être assortie de conditions visant à assurer que les activités prévues dans le cadre de l’exploitation de l’assignation autorisée ne porteront pas atteinte aux intérêts de la sécurité et de la défense nationale ou au respect par la France de ses engagements internationaux ;

- complète 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 par les textes législatifs ou réglementaires. Le renvoi actuel pour l'application de l'article L. 97-2 du CPCE au régime de sanctions de l'article L. 36-11 du même code qui est propre aux compétences de l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse est remplacé par des dispositions propres au pouvoir de sanction du ministre en charge des communications électroniques. Ce dernier pourra ainsi mettre en demeure le titulaire d'une autorisation d'exploitation d'assignation de fréquences 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. Etant précisé que la procédure prévue est respectueuse du principe du contradictoire et que la décision pourra faire l'objet d'un recours de pleine juridiction.
- complète le VI. de l'article L. 97-2 du CPCE, par conformité avec les modifications évoquées ci-avant.

4. ANALYSE DES IMPACTS DES DISPOSITIONS ENVISAGEES

4.1. IMPACTS JURIDIQUES

4.1.1. Impacts sur l'ordre juridique interne

La disposition retenue modifie l'article L. 97-2 du code des postes et des communications électroniques.

4.1.2. Articulation avec le droit international et le droit de l'Union européenne

Les dispositions ne présentent pas d'achoppement avec le droit international et le droit de l'Union européenne. En effet, en premier lieu, le droit de l'Union européen ne traite pas de l'utilisation par les États membres d'assignations de fréquences déposées auprès de l'UIT. En second lieu, si le RR de l'UIT prévoit les conditions dans lesquels les États peuvent déposer auprès de l'UIT et mettre en œuvre des assignations de fréquences, il leur laisse une liberté complète pour permettre à des acteurs privés d'exploiter des assignations déposées en leur nom auprès de l'UIT.

4.2. IMPACTS ECONOMIQUES ET FINANCIERS

4.2.1. Impacts macroéconomiques

Sans objet.

4.2.2. Impacts sur les entreprises

En 2023, l'ANFr a traité 55 demandes de dépôts d'assignations[231]. Elle estime que de l'ordre de trois cas par an seraient susceptibles de faire l'objet d'un contrôle approfondi au titre des nouvelles dispositions.

De même, selon les estimations de l'agence, cette dernière reçoit trois à quatre demandes d'autorisation d'exploitation d'assignation par année. Le nombre de cas susceptibles de faire l'objet d'un contrôle approfondi au titre des nouvelles dispositions sera donc en pratique extrêmement limité.

En conséquence, l'impact sur les entreprises semble réduit à quelques cas particuliers, pour lesquels une instruction complémentaire sera nécessaire. La charge de travail supplémentaire pour les entreprises concernées restera minime comparativement à la charge de travail que représente en l'État l'exploitation d'une assignation déposée par un État auprès de l'UIT (l'entreprise doit notamment s'impliquer dans les travaux de coordination avec les autres utilisateurs d'assignation délivrées par l'UIT). La mesure proposée n'en demeure pas moins nécessaire comme expliqué ci-dessus.

4.2.3. Impacts budgétaires

Impact nul.

4.3. IMPACTS SUR LES COLLECTIVITES TERRITORIALES

Sans objet.

4.4. IMPACTS SUR LES SERVICES ADMINISTRATIFS

La mesure présente un impact mineur sur la procédure à suivre par l'ANFR dans le cadre de l'instruction des demandes de dépôts d'enregistrements auprès de l'UIT et de demande d'autorisation d'exploitation des assignations déposées par la France auprès de l'UIT. Ces modifications n'induisent toutefois pas de changement significatif sur la charge de travail de l'ANFR quant à la conduite de ces procédures.

4.5. IMPACTS SOCIAUX

[231] L'ANFR estime que la moyenne annuelle de demande traitée est de 60 par an.

4.5.1. Impacts sur les personnes en situation de handicap

Sans objet.

4.5.2. Impacts sur l'égalité entre les femmes et les hommes

Sans objet.

4.5.3. Impacts sur la jeunesse

Sans objet.

4.5.4. Impacts sur les professions réglementées

Sans objet.

4.6. IMPACTS SUR LES PARTICULIERS

Sans objet.

4.7. IMPACTS ENVIRONNEMENTAUX

Sans objet.

5. CONSULTATIONS ET MODALITES D'APPLICATION

5.1. CONSULTATIONS MENEES

En application de l'article L. 1212-2 du code général des collectivités territoriales, le présent article a été soumis à l'examen du Conseil national d'évaluation des normes (CNEN), qui a rendu un avis défavorable le 22 mai 2024.

En application de l'article L. 36-5 du code des postes et des communications électroniques, l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse (ARCEP) a été saisie pour avis le 7 mai 2024 sur l'ensemble du projet de loi. Cette dernière a rendu un avis favorable le 23 mai 2024 en ce sens qu'il ne comprend aucune remarque concernant le présent article.

Sur le fondement de l'article 8 de la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, la Commission nationale de l'informatique et des libertés (CNIL) a été consultée à titre facultatif.

La Commission supérieure du numérique et des postes a été consultée à titre facultatif.

5.2. MODALITES D'APPLICATION

5.2.1. Application dans le temps

Cette disposition s'appliquera aux demandes d'assignations de fréquences déposées à partir du lendemain de la publication de la présente loi au *Journal officiel* de la République française afin de permettre aux administrations et aux entreprises concernées de s'adapter au nouveau cadre réglementaire.

5.2.2. Application dans l'espace

Le présent article s'applique en métropole.

Par ailleurs, conformément aux compétences de l'Etat en matière d'assignation de fréquences l'article est applicable de plein droit dans les collectivités relevant de l'article 73 de la Constitution (Guadeloupe, Guyane, Martinique, Mayotte, La Réunion).

Il est également applicable dans les collectivités relevant de l'article 74 de la Constitution (Saint-Barthélemy, Saint-Martin, Saint-Pierre-et-Miquelon, îles Wallis et Futuna, Polynésie française) eu égard à leurs lois organiques respectives.

Il est applicable en Nouvelle-Calédonie régie par le titre XIII de la Constitution.

Il est, enfin, applicable dans les Terres australes et antarctiques françaises.

L'article L. 97-4 du code des postes et des communications électroniques prévoit d'ores et déjà cette applicabilité expresse « *en Nouvelle-Calédonie, en Polynésie française, à Wallis-et-Futuna et dans les Terres australes et antarctiques françaises*. »

5.2.3. Textes d'application

Le texte nécessitera la prise d'un décret en Conseil d'Etat portant sur les articles R. 52-3-1 et suivants du CPCE.

TITRE III – RESILIENCE OPERATIONNELLE NUMERIQUE DU SECTEUR FINANCIER

CHAPITRE IER – DISPOSITIONS MODIFIANT LE CODE MONETAIRE ET FINANCIER

Article 43 – Modification de la définition des prestataires de services techniques

1. ÉTAT DES LIEUX

1.1. CADRE GENERAL

La directive (UE) 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015 concernant les services de paiement dans le marché intérieur (« DSP2 »)[232] régit la fourniture de services de paiement à des utilisateurs. La fourniture de tels services requiert un agrément en tant que prestataire de services de paiement (en tant qu'établissement de crédit, d'établissement de paiement ou d'établissement de monnaie électronique), sauf exemptions prévues par la directive.

La fourniture de services de paiement à des utilisateurs s'appuie sur des services de nature technique qui ne constituent pas des services de paiement au sens de la DSP2. Cette directive effectue une distinction entre les services de paiement, limitativement énumérés à son annexe I et dont la fourniture requiert un agrément, et les services techniques, qui ne requièrent pas d'agrément spécifique.

En ce sens, la directive exclut de son champ d'application, au paragraphe j) de son article 3, les « services fournis par des prestataires de services techniques à l'appui de la fourniture de services de paiement, sans qu'ils entrent, à aucun moment, en possession des fonds à transférer ». Il s'agit donc d'acteurs fournissant des services support à l'exécution d'opérations de paiement.

[232] 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.

Selon la liste non limitative fournie par la DSP2, ces services techniques consistent notamment dans le traitement et l'enregistrement des données, les services de protection de la confiance de la vie privée, l'authentification des données et des entités, les technologies de l'information et la fourniture de réseaux de communication, ainsi que la fourniture et la maintenance des terminaux et dispositifs utilisés aux fins des services de paiement, à l'exception des services d'initiation de paiement et des services d'information sur les comptes.

1.2. CADRE CONSTITUTIONNEL

Aux termes de l'article 88-1 de la Constitution : « La République participe aux Communautés européennes et à l'Union européenne, constituées d'Etats qui ont choisi librement, en vertu des traités qui les ont instituées, d'exercer en commun certaines de leurs compétences ». Le Conseil constitutionnel déduit de cette disposition que « la transposition en droit interne d'une directive communautaire résulte d'une exigence constitutionnelle »[233]. Il en va de même pour une loi ayant pour objet d'adapter le droit interne à un règlement de l'Union européenne[234].

1.3. CADRE CONVENTIONNEL

Le 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 (« règlement DORA ») fixe des exigences uniformes en matière de sécurité des réseaux et des systèmes d'informations des entités financières, afin de leur permettre de mettre en place les garanties nécessaires face aux perturbations ou menaces impliquant les technologies de l'information et de la communication (TIC). Ce règlement fixe un cadre harmonisé en matière de gestion des risques liés aux TIC qui remplace les cadres existants fixés par les directives sectorielles, y compris, en matière de paiement, par la DSP2.

En conséquence, la directive (UE) 2022/2556 du Parlement européen et du Conseil du 14 décembre 2022 modifiant les directives 2009/65/CE, 2009/138/CE, 2011/61/UE, 2013/36/UE, 2014/59/UE, 2014/65/UE, (UE) 2015/2366 et (UE) 2016/2341 en ce qui concerne la résilience opérationnelle numérique du secteur financier (« directive DORA ») modifie plusieurs directives sectorielles.

---

[233] Voir notamment la décision n° 2004-496 DC du 10 juin 2004, « Loi pour la confiance dans l'économie numérique ».

[234] Voir par exemple la décision n° 2018-765, « Loi relative à la protection des données personnelles », considérant 3.

L'article 7(1) de la directive DORA amende la définition des prestataires de services techniques figurant à l'article 3, point (j) de la DSP2 afin d'y inclure les services de fourniture de technologies de l'information et de la communication (TIC) dont les risques sont désormais uniformément couverts par le règlement DORA.

1.4. ÉLEMENTS DE DROIT COMPARE

Les autres Etats membres de l'Union européenne modifieront également leur définition des prestataires de services techniques, conformément à la directive DORA.

2. NECESSITE DE LEGIFERER ET OBJECTIFS POURSUIVIS

2.1. NECESSITE DE LEGIFERER

La nécessité de légiférer provient ici de l'obligation constitutionnelle de transposition en droit interne d'une directive imposée par l'article 88-1 de la Constitution qui dispose que « [l]a République participe à l'Union européenne ». Cette obligation a d'ailleurs été rappelée par le Conseil constitutionnel dans le considérant 7 de sa décision n° 2004-496 DC du 10 juin 2004 : « Considérant qu'aux termes de l'article 88-1 de la Constitution […] ; qu'ainsi, la transposition en droit interne d'une directive communautaire résulte d'une exigence constitutionnelle à laquelle il ne pourrait être fait obstacle qu'en raison d'une disposition expresse contraire de la Constitution ».

2.2. OBJECTIFS POURSUIVIS

Cet article permet de transposer dans le code monétaire et financier l'article 7 (1) de la directive DORA, qui modifie la définition des services fournis par des prestataires de services techniques à l'appui de la fourniture de services de paiement prévue dans la deuxième directive sur les services de paiement[235].

3. OPTIONS POSSIBLES ET DISPOSITIF RETENU

3.1. OPTIONS ENVISAGEES

[235] Directive (UE) 2015/2366 ou DSP2.

Aucune autre option n'a été envisagée dans la mesure où cette disposition est commandée par une norme supérieure issue du droit de l'Union européenne.

3.2. OPTION RETENUE

La directive DORA ne prévoit que des modifications d'ordre technique des différentes directives sectorielles en matière financière, notamment la directive sur les services de paiement de 2015, qui visent à assurer la cohérence avec les nouvelles exigences introduites par le règlement DORA.

Dans un souci de simplicité et dans la mesure où la transposition consistera en une modification de la définition des prestataires de services techniques fournie à l'article 3, point (j) de la directive DPS2, il a été décidé de modifier à l'identique l'article L. 314-1 du code monétaire et financier la rédaction adoptée à l'article 7(1) de la directive DORA modifiant la directive DSP2.

4. ANALYSE DES IMPACTS DES DISPOSITIONS ENVISAGEES

4.1. IMPACTS JURIDIQUES

4.1.1. Impacts sur l'ordre juridique interne

L'article L. 314-1 du code monétaire et financier est modifié.

4.1.2. Articulation avec le droit international et le droit de l'Union européenne

Cette disposition vise à modifier le code monétaire et financier afin de prendre en considération les modifications apportées par l'article 7 (1) de la directive DORA susmentionnée, qui modifie elle-même la directive DPS2.

4.2. IMPACTS ECONOMIQUES ET FINANCIERS

4.2.1. Impacts macroéconomiques

Néant.

4.2.2. Impacts sur les entreprises

Néant.

4.2.3. Impacts budgétaires

Néant.

4.3. IMPACTS SUR LES COLLECTIVITES TERRITORIALES

Néant. S'agissant d'articles relatifs au droit monétaire, bancaire et financier, le présent article est sans incidence sur le fonctionnement des collectivités territoriales.

4.4. IMPACTS SUR LES SERVICES ADMINISTRATIFS

Néant.

4.5. IMPACTS SOCIAUX

4.5.1. Impacts sur la société

Néant.

4.5.2. Impacts sur les personnes en situation de handicap

Néant.

4.5.3. Impacts sur l'égalité entre les femmes et les hommes

Néant.

4.5.4. Impacts sur la jeunesse

Néant.

4.5.5. Impacts sur les professions réglementées

Néant.

4.6. IMPACTS SUR LES PARTICULIERS

Néant.

4.7. IMPACTS ENVIRONNEMENTAUX

Néant.

5. CONSULTATIONS ET MODALITES D'APPLICATION

5.1. CONSULTATIONS MENEES

En application de l'article L. 614-2 du code monétaire et financier, le Comité consultatif de la législation et de la réglementation financières (CCLRF) a été consulté a rendu un avis favorable le 23 mai 2024.

La rédaction proposée a en outre été envoyée pour information et sur base informelle aux services du Secrétariat général de l'Autorité de contrôle prudentiel et de résolution (ACPR).

5.2. MODALITES D'APPLICATION

5.2.1. Application dans le temps

Le présent article s'appliquera à compter du 17 janvier 2025 conformément à l'article 62 du présent projet de loi.

5.2.2. Application dans l'espace

La mesure s'applique à l'ensemble du territoire de la République.

Elle s'applique de plein droit aux collectivités territoriales régies par l'article 73 de la Constitution (Guadeloupe, Guyane, Martinique, La Réunion et Mayotte) et certaines des collectivités relevant de l'article 74 (Saint-Barthélemy, Saint Martin et Saint-Pierre-et-Miquelon).

L'article 4 de la loi du 29 juillet 1961, l'article 7 de la loi organique n° 2004-192 du 27 février 2004 portant statut d'autonomie de la Polynésie Française et l'article 6-2 de la loi n° 99-209 organique du 19 mars 1999 relative à la Nouvelle-Calédonie soumettent respectivement pour les Îles Wallis et Futuna, la Polynésie Française et la Nouvelle-Calédonie au principe de spécialité législative, les lois et règlements n'y étant applicables que sur mention expresse, dès lors qu'ils interviennent dans un domaine pour lequel l'Etat est compétent. En effet, l'Etat est compétent en matière bancaire et financière dans ces collectivités ultramarines régies par le principe de spécialité législative où toute création ou modification du code précité doit être rendue applicable par mention expresse.

Ainsi, l'article 56 du projet de loi rend applicables les présentes dispositions en Nouvelle-Calédonie, en Polynésie française et dans les îles Wallis et Futuna en modifiant les articles L. 752-10, L. 753-10 et L. 754-8 du code monétaire et financier.

5.2.3. Textes d'application

Le présent article ne requiert aucune mesure d'application.

Article 44 – Maintien de la résilience opérationnelle des gestionnaires de plateformes de négociation

1. ÉTAT DES LIEUX

1.1. CADRE GENERAL

L'article L. 420-3 du code monétaire et financier décrit les exigences organisationnelles des gestionnaires de plateformes de négociation, afin d'en assurer la résilience de ces plateformes y compris en période de tension sur les marchés. Une plateforme de négociation est un marché réglementé au sens de l'article L. 421-1 du code monétaire et financier, un système multilatéral de négociation au sens de l'article L. 424-1 ou un système organisé de négociation au sens de l'article L. 425-1.

Le I de l'article L. 420-3 du code monétaire et financier précise les obligations relatives aux systèmes et procédures mis en place par les gestionnaires de plateformes de négociation pour en assurer la résilience et la capacité à gérer de grands volumes d'ordres.

Le III de l'article L. 420-3 du code monétaire et financier décrit les exigences des gestionnaires de plateformes de négociation vis-à-vis des personnes utilisant des systèmes de négociation algorithmique afin de réaliser des transactions sur ces plateformes, notamment pour s'assurer que celles-ci ne participent pas à perturber le bon fonctionnement des marchés.

1.2. CADRE CONSTITUTIONNEL

Aux termes de l'article 88-1 de la Constitution : « La République participe aux Communautés européennes et à l'Union européenne, constituées d'Etats qui ont choisi librement, en vertu des traités qui les ont instituées, d'exercer en commun certaines de leurs compétences ». Le Conseil constitutionnel déduit de cette disposition que : « la transposition en droit interne d'une directive communautaire résulte d'une exigence constitutionnelle »[236] . Il en va de même pour une loi ayant pour objet d'adapter le droit interne à un règlement de l'Union européenne[237].

1.3. CADRE CONVENTIONNEL

[236] Voir notamment la décision n° 2004-496 DC du 10 juin 2004, « Loi pour la confiance dans l'économie numérique ».

[237] Voir par exemple la décision n° 2018-765, « Loi relative à la protection des données personnelles », considérant 3.

Le 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 (« règlement DORA ») fixe des exigences uniformes en matière de sécurité des réseaux et des systèmes d'informations des entités financières, afin de leur permettre de mettre en place les garanties nécessaires face aux perturbations ou menaces impliquant les technologies de l'information et de la communication (TIC). Ce règlement fixe un cadre harmonisé en matière de gestion des risques liés aux TIC qui remplace les cadres existants fixés par les directives sectorielles, y compris, s'agissant des marchés d'instruments financiers, par la directive 2014/65/UE (MIFID II).

En conséquence, la directive (UE) 2022/2556 du Parlement européen et du Conseil du 14 décembre 2022 modifiant les directives 2009/65/CE, 2009/138/CE, 2011/61/UE, 2013/36/UE, 2014/59/UE, 2014/65/UE, (UE) 2015/2366 et (UE) 2016/2341 en ce qui concerne la résilience opérationnelle numérique du secteur financier (« directive DORA ») modifie plusieurs directives sectorielles.

L'article 6.4.a) de la directive DORA modifie les exigences en matière de mise en œuvre et de maintien de la résilience opérationnelle des marchés règlementés figurant à l'article 48 la directive MiFID II.

1.4. ÉLEMENTS DE DROIT COMPARE

Les autres Etats membres devront également transposer cette directive en droit national.

2. NECESSITE DE LEGIFERER ET OBJECTIFS POURSUIVIS

2.1. NECESSITE DE LEGIFERER

La nécessité de légiférer provient ici de l'obligation constitutionnelle de transposition en droit interne d'une directive imposée par l'article 88-1 de la Constitution qui dispose que « [l]a République participe à l'Union européenne ». Cette obligation a d'ailleurs été rappelée par le Conseil constitutionnel dans le considérant 7 de sa décision n° 2004-496 DC du 10 juin 2004 : « Considérant qu'aux termes de l'article 88-1 de la Constitution […] ; qu'ainsi, la transposition en droit interne d'une directive communautaire résulte d'une exigence constitutionnelle à laquelle il ne pourrait être fait obstacle qu'en raison d'une disposition expresse contraire de la Constitution ».

2.2. OBJECTIFS POURSUIVIS

Cet article permet de transposer dans le code monétaire et financier l'article 6.4.a) de la directive DORA, en précisant les modalités de mise en œuvre de la résilience opérationnelle par les gestionnaires de plateformes de négociation.

3. OPTIONS POSSIBLES ET DISPOSITIF RETENU

3.1. OPTIONS ENVISAGEES

Aucune autre option n'a été envisagée dans la mesure où cette disposition est commandée par une norme supérieure issue du droit de l'Union européenne.

3.2. OPTION RETENUE

La directive DORA ne prévoit que des modifications d'ordre technique des différentes directives sectorielles qui visent à assurer la cohérence avec les nouvelles exigences introduites par le règlement DORA. Dans un souci de simplicité, il a été décidé de reproduire à l'identique dans l'article L. 420-3 du code monétaire et financier la rédaction adoptée à l'article 6.4.a de la directive DORA modifiant la directive MiFID II.

Ainsi, le présent article modifie l'article L. 420-3 du code monétaire et financier relatif aux systèmes, procédures et mécanismes mis en place par les gestionnaires de plateformes de négociation afin de s'assurer que ceux-ci soient 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. Il est proposé d'amender cet article afin notamment de préciser que les gestionnaires de plateformes de négociation ceux-ci doivent assurer et maintenir leur résilience opérationnelle, et de faire référence au règlement DORA.

Dans le détail, il est proposé de modifier le I de l'article L. 420-3 du code monétaire et financier pour y introduire une référence aux exigences fixées par le règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier (règlement DORA) s'agissant des conditions de maintien de la résilience opérationnelle des plateformes de négociation et des plans de continuité des activités mises en œuvre. Il est également prévu une modification du III du même article afin d'y introduire une référence au règlement DORA s'agissant des environnements de tests réalisés par les personnes utilisant des systèmes de négociation algorithmique.

4. ANALYSE DES IMPACTS DES DISPOSITIONS ENVISAGEES

4.1. IMPACTS JURIDIQUES

4.1.1. Impacts sur l'ordre juridique interne

L'article L. 420-3 du code monétaire et financier est modifié.

4.1.2. Articulation avec le droit international et le droit de l'Union européenne

La rédaction proposée reprend *in extenso* celle adoptée à l'article 6.4.a de la directive DORA.

4.2. IMPACTS ECONOMIQUES ET FINANCIERS

4.2.1. Impacts macroéconomiques

Néant.

4.2.2. Impacts sur les entreprises

Les opérateurs de plateformes de négociation doivent mettre à jour conformément aux exigences fixées au chapitre II du règlement (UE) 2022/2554 leur cadre de gouvernance et de contrôle interne pour établir les responsabilités de supervision et les modalités d'exercice du suivi de la gestion du risque. De même, elles doivent actualiser le cadre de gestion du risque lié aux TIC conformément aux exigences de la section II du même chapitre pour garantir la résilience opérationnelle numérique des systèmes.

4.2.3. Impacts budgétaires

Néant.

4.3. IMPACTS SUR LES COLLECTIVITES TERRITORIALES

Néant. S'agissant d'articles relatifs au droit monétaire, bancaire et financier, le présent article est sans incidence sur le fonctionnement des collectivités territoriales.

4.4. IMPACTS SUR LES SERVICES ADMINISTRATIFS

Néant.

4.5. IMPACTS SOCIAUX

4.5.1. Impacts sur la société

Néant.

4.5.2. Impacts sur les personnes en situation de handicap

Néant.

4.5.3. Impacts sur l'égalité entre les femmes et les hommes

Néant.

4.5.4. Impacts sur la jeunesse

Néant.

4.5.5. Impacts sur les professions réglementées

Néant.

4.6. IMPACTS SUR LES PARTICULIERS

Néant.

4.7. IMPACTS ENVIRONNEMENTAUX

Néant.

5. CONSULTATIONS ET MODALITES D'APPLICATION

5.1. CONSULTATIONS MENEES

En application de l'article L. 614-2 du code monétaire et financier, le Comité consultatif de la législation et de la réglementation financières (CCLRF) a été consulté a rendu un avis favorable le 23 mai 2024.

La rédaction proposée a en outre été envoyée pour information et sur base informelle à l'Autorité des marchés financiers, qui a contribué à sa préparation.

5.2. MODALITES D'APPLICATION

5.2.1. Application dans le temps

Le présent article s'appliquera à compter du 17 janvier 2025 conformément à l'article 62 du présent projet de loi.

5.2.2. Application dans l'espace

La mesure s'applique à l'ensemble du territoire de la République.

Elle s'applique de plein droit aux collectivités territoriales régies par l'article 73 de la Constitution (Guadeloupe, Guyane, Martinique, La Réunion et Mayotte) et certaines des collectivités relevant de l'article 74 (Saint-Barthélemy, Saint Martin et Saint-Pierre-et-Miquelon).

L'article 4 de la loi du 29 juillet 1961, l'article 7 de la loi organique n° 2004-192 du 27 février 2004 portant statut d'autonomie de la Polynésie Française et l'article 6-2 de la loi n° 99-209 organique du 19 mars 1999 relative à la Nouvelle-Calédonie soumettent respectivement pour les Îles Wallis et Futuna, la Polynésie Française et la Nouvelle-Calédonie au principe de spécialité législative, les lois et règlements n'y étant applicables que sur mention expresse, dès lors qu'ils interviennent dans un domaine pour lequel l'Etat est compétent. En effet, l'Etat est compétent en matière bancaire et financière dans ces collectivités ultramarines régies par le principe de spécialité législative où toute création ou modification du code précité doit être rendue applicable par mention expresse.

Ainsi, l'article 56 du projet de loi rend applicables les présentes dispositions en Nouvelle-Calédonie, en Polynésie française et dans les îles Wallis et Futuna en modifiant les articles L. 762-3, L. 763-3 et L. 764-3 du code monétaire et financier.

Enfin, la modification de l'article L. 712-7 du code monétaire et financier réalisée par l'article 56 du projet de loi rend applicable le règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier à Saint-Pierre et Miquelon, en Nouvelle-Calédonie, en Polynésie française et dans les îles Wallis et Futuna qui sont des pays et territoires d'outre-mer où le droit de l'Union européenne ne s'applique pas.

Par coordination, l'article L. 761-1 est complété par les références au règlement (UE) 2022/2554 précité.

5.2.3. Textes d'application

La présente disposition ne requiert aucune mesure d’application.

Article 45 – Gestion du risque lié aux technologies de l'information et de la communication par les entreprises de marché

1. ÉTAT DES LIEUX

1.1. CADRE GENERAL

L'article L. 421-11 du CMF définit les dispositions devant être prises par les entreprises de marché, c'est-à-dire les sociétés gérant un marché règlementé, afin de garantir le bon fonctionnement des marchés et de disposer de procédures d'urgence destinées à faire face à d'éventuels dysfonctionnements. Celles-ci doivent être capables de détecter, prévenir et gérer tout dysfonctionnement d'ampleur affectant le bon fonctionnement du marché réglementé et portant atteinte aux intérêts des membres du marché. A ce titre, les sociétés gestionnaires doivent disposer en permanence des moyens et de l'organisation leur permettant d'identifier les risques majeurs et d'en atténuer les conséquences. Des procédures d'urgence doivent ainsi être prévues pour faciliter le dénouement des transactions exécutées dans leurs systèmes.

1.2. CADRE CONSTITUTIONNEL

Aux termes de l'article 88-1 de la Constitution : « La République participe aux Communautés européennes et à l'Union européenne, constituées d'Etats qui ont choisi librement, en vertu des traités qui les ont instituées, d'exercer en commun certaines de leurs compétences ». Le Conseil constitutionnel déduit de cette disposition que : « la transposition en droit interne d'une directive communautaire résulte d'une exigence constitutionnelle »[238]. Il en va de même pour une loi ayant pour objet d'adapter le droit interne à un règlement de l'Union européenne[239].

1.3. CADRE CONVENTIONNEL

Le 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 (« règlement DORA ») fixe des exigences uniformes en matière de sécurité des réseaux et des

[238] Voir notamment la décision n° 2004-496 DC du 10 juin 2004, « Loi pour la confiance dans l'économie numérique ».

[239] Voir par exemple la décision n° 2018-765, « Loi relative à la protection des données personnelles », considérant 3.

systèmes d'informations des entités financières, afin de leur permettre de mettre en place les garanties nécessaires face aux perturbations ou menaces impliquant les technologies de l'information et de la communication (TIC). Ce règlement fixe un cadre harmonisé en matière de gestion des risques liés aux TIC qui remplace les cadres existants fixés par les directives sectorielles, y compris, s'agissant des marchés d'instruments financiers, par la directive 2014/65/UE (MIFID II).

En conséquence, la directive (UE) 2022/2556 du Parlement européen et du Conseil du 14 décembre 2022 modifiant les directives 2009/65/CE, 2009/138/CE, 2011/61/UE, 2013/36/UE, 2014/59/UE, 2014/65/UE, (UE) 2015/2366 et (UE) 2016/2341 en ce qui concerne la résilience opérationnelle numérique du secteur financier (« directive DORA ») modifie plusieurs directives sectorielles.

L'article 6.3 de la directive DORA amende la directive MiFID II afin de préciser que les entreprises de marché doivent disposer de moyens leur permettant de gérer les risques TIC conformément au chapitre II du règlement DORA, et de supprimer le 4 de l'article L. 421-11 du code monétaire et financier conformément au b) de l'article 6 paragraphe 3 de la directive DORA.

1.4. ÉLEMENTS DE DROIT COMPARE

Les autres Etats membres devront également transposer cette directive en droit national.

2. NECESSITE DE LEGIFERER ET OBJECTIFS POURSUIVIS

2.1. NECESSITE DE LEGIFERER

La nécessité de légiférer provient ici de l'obligation constitutionnelle de transposition en droit interne d'une directive imposée par l'article 88-1 de la Constitution qui dispose que « [l]a République participe à l'Union européenne ». Cette obligation a d'ailleurs été rappelée par le Conseil constitutionnel dans le considérant 7 de sa décision n° 2004-496 DC du 10 juin 2004 : « Considérant qu'aux termes de l'article 88-1 de la Constitution […] ; qu'ainsi, la transposition en droit interne d'une directive communautaire résulte d'une exigence constitutionnelle à laquelle il ne pourrait être fait obstacle qu'en raison d'une disposition expresse contraire de la Constitution ».

2.2. OBJECTIFS POURSUIVIS

Le présent article permet de transposer à l'article L. 421-11 du code monétaire et financier relatif aux obligations de l'entreprise de marché les exigences introduites par les chapitres II

et IV du règlement DORA en matière de gestion des risques liés aux technologies de l'information et de la communication.

3. OPTIONS POSSIBLES ET DISPOSITIF RETENU

3.1. OPTIONS ENVISAGEES

Aucune autre option n'a été envisagée dans la mesure où cette disposition est commandée par une norme supérieure issue du droit de l'Union européenne.

3.2. OPTION RETENUE

La directive DORA ne prévoit que des modifications d'ordre technique des différentes directives sectorielles qui visent à assurer la cohérence avec les nouvelles exigences introduites par le règlement DORA. Il a été décidé de modifier l'article L. 421-11 en introduisant dans le I.2. l'obligation pour l'entreprise de marché de prendre les dispositions nécessaires en vue de gérer les risques auxquels elle est exposée, y compris les risques liés aux TIC conformément au chapitre II du règlement DORA. Le 4. est supprimé pour transposer le 3) b) de l'article 6 de la directive DORA.

4. ANALYSE DES IMPACTS DES DISPOSITIONS ENVISAGEES

4.1. IMPACTS JURIDIQUES

4.1.1. Impacts sur l'ordre juridique interne

La présente disposition modifie l'article L. 421-11 du code monétaire et financier.

4.1.2. Articulation avec le droit international et le droit de l'Union européenne

La présente disposition est conforme au droit de l'Union européenne, reprenant la rédaction formulée à l'article 6.3 de la directive DORA.

4.2. IMPACTS ECONOMIQUES ET FINANCIERS

4.2.1. Impacts macroéconomiques

Néant.

4.2.2. Impacts sur les entreprises

Les entités financières doivent actualiser leur cadre de gouvernance et d'organisation interne ainsi que leur cadre de gestion du risque lié aux TIC pour garantir un contrôle interne du risque prudent et efficace conformément aux exigences détaillées dans le chapitre II du règlement DORA. Elles doivent également modifier leurs systèmes de contrôle des risques afin de prendre en compte les exigences générales applicables à la réalisation des tests de résilience opérationnelle numérique prévues par le chapitre IV du règlement DORA.

4.2.3. Impacts budgétaires

Néant.

4.3. IMPACTS SUR LES COLLECTIVITES TERRITORIALES

Néant. S'agissant d'articles relatifs au droit monétaire, bancaire et financier, le présent article est sans incidence sur le fonctionnement des collectivités territoriales.

4.4. IMPACTS SUR LES SERVICES ADMINISTRATIFS

Néant.

4.5. IMPACTS SOCIAUX

4.5.1. Impacts sur la société

Néant.

4.5.2. Impacts sur les personnes en situation de handicap

Néant.

4.5.3. Impacts sur l'égalité entre les femmes et les hommes

Néant.

4.5.4. Impacts sur la jeunesse

Néant.

4.5.5. Impacts sur les professions réglementées

Néant.

4.6. IMPACTS SUR LES PARTICULIERS

Néant.

4.7. IMPACTS ENVIRONNEMENTAUX

Néant.

5. CONSULTATIONS ET MODALITES D'APPLICATION

5.1. CONSULTATIONS MENEES

En application de l'article L. 614-2 du code monétaire et financier, le Comité consultatif de la législation et de la réglementation financières (CCLRF) a été consulté a rendu un avis favorable le 23 mai 2024.

La rédaction proposée a en outre été envoyée pour information et sur base informelle à l'Autorité des marchés financiers, qui a contribué à sa préparation.

5.2. MODALITES D'APPLICATION

5.2.1. Application dans le temps

Le présent article s'appliquera à compter du 17 janvier 2025 conformément à l'article 62 du présent projet de loi.

5.2.2. Application dans l'espace

La mesure s'applique à l'ensemble du territoire de la République.

Elle s'applique de plein droit aux collectivités territoriales régies par l'article 73 de la Constitution (Guadeloupe, Guyane, Martinique, La Réunion et Mayotte) et certaines des collectivités relevant de l'article 74 (Saint-Barthélemy, Saint Martin et Saint-Pierre-et-Miquelon).

L’article 4 de la loi du 29 juillet 1961, l’article 7 de la loi organique n° 2004-192 du 27 février 2004 portant statut d’autonomie de la Polynésie Française et l’article 6-2 de la loi n° 99-209 organique du 19 mars 1999 relative à la Nouvelle-Calédonie soumettent respectivement pour les Îles Wallis et Futuna, la Polynésie Française et la Nouvelle-Calédonie au principe de spécialité législative, les lois et règlements n’y étant applicables que sur mention expresse, dès lors qu’ils interviennent dans un domaine pour lequel l’Etat est compétent. En effet, l’Etat est compétent en matière bancaire et financière dans ces collectivités ultramarines régies par le principe de spécialité législative où toute création ou modification du code précité doit être rendue applicable par mention expresse.

Ainsi, l’article 56 du projet de loi rend applicables les présentes dispositions en Nouvelle-Calédonie, en Polynésie française et dans les îles Wallis et Futuna en modifiant les articles L. 762-4, L. 763-4 et L. 764-3 du code monétaire et financier.

Enfin, la modification de l’article L. 712-7 du code monétaire et financier réalisée par l’article 56 du projet de loi rend applicable le règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier à Saint-Pierre et Miquelon, en Nouvelle-Calédonie, en Polynésie française et dans les îles Wallis et Futuna qui sont des pays et territoires d’outre-mer où le droit de l’Union européenne ne s’applique pas.

Par coordination, l’article L. 761-1 est complété par les références au règlement (UE) 2022/2554 précité.

5.2.3. Textes d’application

La présente disposition ne requiert aucune mesure d’application.

Article 46 – Références aux risques liés aux technologies de l'information et de la communication au sein des dispositifs de gestion des risques des établissements de crédit et des sociétés de financement

1. ÉTAT DES LIEUX

1.1. CADRE GENERAL

L'utilisation généralisée de systèmes de technologies de l'information et de la communication (TIC) – à l'instar des réseaux, des infrastructures numériques, des actifs logiciels ou des dispositifs de sauvegarde –, une numérisation et une connectivité poussées constituent désormais des caractéristiques essentielles des activités des entités financières françaises. A l'aune de ce constat, le 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, ci-après « règlement DORA », renforce les obligations opérationnelles s'imposant aux principaux acteurs du secteur financier. Il est complété par la 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, ci-après « directive DORA » qui regroupe une série de dispositions techniques, visant à clarifier les obligations et à actualiser les références de directives en droit interne.

Concernant les établissements de crédit, tels que définis au I de l'article L. 511-1 du code monétaire et financier, la 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, modifiant la directive 2002/87/CE et abrogeant les directives 2006/48/CE et 2006/49/CE (ci-après « CRD ») n'énonce actuellement que des règles générales de gouvernance interne et des dispositions relatives au risque opérationnel définissant, à l'article L. 511-41-1-B du code monétaire et financier, des exigences en matière de plans d'urgence et de poursuite de l'activité qui servent implicitement de base pour traiter le risque lié aux technologies de l'information et de la communication (TIC). Ces risqués liés aux TIC incluent notamment la survenance d'incidents opérationnels au sein des systèmes d'information des entités financières pouvant affecter négativement la continuité de leurs activités et leurs clients, ainsi que la dépendance des entités financières à l'égard de prestataires tiers de services de TIC auprès desquels celles-ci ont sous-traité une partie de

leurs fonctions ou activités. Afin de traiter explicitement et clairement les risques liés aux TIC, l'article 4(3) de la directive DORA[240] modifie dans la directive CRD les exigences en matière de plans d'urgence et de poursuite de l'activité de manière à inclure également « les politiques et plans d'urgence et de poursuite de l'activité » ainsi que des « plans de réponse et de rétablissement » en ce qui concerne le risque lié aux TIC, conformément aux exigences fixées dans le règlement DORA. Le contenu de ces politiques et plans, lorsqu'ils visent spécifiquement les risques liés aux TIC, devra être précisé par des normes techniques de réglementation en cours de développement auprès des autorités européennes de surveillance (mandatées à cette fin sur la base de l'article 15 du règlement DORA).

Ces modifications doivent donc être introduites dans les dispositions de droit interne transposant la directive sectorielle CRD applicable aux établissements de crédit (article L. 511-41-1-B du code monétaire et financier).

1.2. CADRE CONSTITUTIONNEL

Aux termes de l'article 88-1 de la Constitution : « La République participe aux Communautés européennes et à l'Union européenne, constituées d'Etats qui ont choisi librement, en vertu des traités qui les ont instituées, d'exercer en commun certaines de leurs compétences ». Le Conseil constitutionnel déduit de cette disposition que : « la transposition en droit interne d'une directive communautaire résulte d'une exigence constitutionnelle »[241]. Il en va de même pour une loi ayant pour objet d'adapter le droit interne à un règlement de l'Union européenne[242].

En tout état de cause, la mesure relève du domaine de la loi en application de l'article 34 de la Constitution, au titre des obligations civiles et commerciales.

1.3. CADRE CONVENTIONNEL

Le règlement européen DORA (UE) 2022/2554 du Parlement européen et du Conseil, adopté à l'automne 2022 et entré en vigueur le 16 janvier 2023, renforce les obligations opérationnelles s'imposant aux principaux acteurs du secteur financier. Il est complété par la directive éponyme qui regroupe une série de dispositions techniques, visant à clarifier les

---

[240] 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.

[241] Voir notamment la décision n° 2004-496 DC du 10 juin 2004, « Loi pour la confiance dans l'économie numérique ».

[242] Voir par exemple la décision n° 2018-765, « Loi relative à la protection des données personnelles », considérant 3.

obligations et à actualiser les références aux enjeux de résilience opérationnelle au sein des directives qui préexistaient au règlement DORA.

L'article 4 de la directive DORA liste les amendements apportés à la directive CRD relative encadrant les activités des établissements de crédit et harmonisant leur surveillance prudentielle.

En sus de la directive CRD, la directive DORA apporte également des modifications à sept autres directives sectorielles :

- la 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 (dite « OPCVM ») ;
- 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 (dite « Solvabilité II ») ;
- la 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 (dite « AIFM ») ;
- la 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 (dite « BRRD ») ;
- la 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 (dite « MIFID ») ;
- la directive (UE) 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015 concernant les services de paiement dans le marché intérieur, modifiant les directives 2002/65/CE, 2009/110/CE et 2013/36/UE et le règlement (UE) no 1093/2010, et abrogeant la directive 2007/64/CE (dite « PSD ») ;
- la directive (UE) 2016/2341 du Parlement européen et du Conseil du 14 décembre 2016 concernant les activités et la surveillance des institutions de retraite professionnelle (dite « IRP »).

1.4. ÉLEMENTS DE DROIT COMPARE

Les autres Etats membres de l'Union européenne modifieront également leur droit national conformément à la directive DORA afin d'introduire une référence aux risques liés aux technologies de l'information et de la communication au sein des dispositifs de gestion des risques des établissements de crédit.

2. NECESSITE DE LEGIFERER ET OBJECTIFS POURSUIVIS

2.1. NECESSITE DE LEGIFERER

La nécessité de légiférer provient ici tout d'abord de l'obligation constitutionnelle de transposition en droit interne d'une directive imposée par l'article 88-1 de la Constitution qui dispose que « [l]a République participe à l'Union européenne ». Cette obligation a d'ailleurs été rappelée par le Conseil constitutionnel dans le considérant 7 de sa décision n° 2004-496 DC du 10 juin 2004 : « Considérant qu'aux termes de l'article 88-1 de la Constitution […] ; qu'ainsi, la transposition en droit interne d'une directive communautaire résulte d'une exigence constitutionnelle à laquelle il ne pourrait être fait obstacle qu'en raison d'une disposition expresse contraire de la Constitution ».

Cet article vise à transposer dans le code monétaire et financier les dispositions des articles 4(3) et 4(4) de la directive DORA, qui modifient respectivement les dispositions de l'article 85(2) de CRD relatives aux plans d'urgence et de poursuite de l'activité et l'article 97(1) de CRD relatif au SREP. Il étend également ces exigences aux sociétés de financement.

2.2. OBJECTIFS POURSUIVIS

Au vu du caractère central de l'utilisation des TIC dans la fourniture de services financiers (à l'instar des réseaux, des infrastructures numériques, des actifs logiciels ou des dispositifs de sauvegarde) et son importance cruciale dans l'exécution des fonctions quotidiennes typiques des entités financières, l'application de ces dispositions permettant la mise en œuvre d'un cadre robuste de résilience opérationnelle numérique est étendue aux sociétés de financement. Cette application des exigences de la directive et du règlement DORA aux sociétés de financement permet en outre de préserver la comparabilité en termes de solidité des régimes applicables respectivement aux établissements de crédit et aux sociétés de financement, condition prévue à l'article 119 du règlement CRR nécessaire au maintien d'un traitement prudentiel plus favorable pour les expositions sur les sociétés de financement.

3. OPTIONS POSSIBLES ET DISPOSITIF RETENU

3.1. OPTIONS ENVISAGEES

Suivant le principe du parallélisme des formes, une disposition législative ne peut être modifiée que par une mesure de même niveau normatif. Ainsi, aucune autre option que le recours à la loi n'a été envisagée ici.

3.2. OPTION RETENUE

La directive DORA ne prévoit que des modifications d'ordre technique des différentes directives sectorielles qui visent à assurer la cohérence avec les nouvelles exigences introduites par le règlement DORA. Dans un souci de simplicité et dans la mesure où la transposition de cette directive DORA est sans enjeu majeur, il a été décidé d'introduire les modifications afférentes dans les dispositions de droit interne transposant la directive sectorielle CRD applicable aux établissements de crédit (article L. 511-41-1-B du code monétaire et financier). Ces dispositions de droit interne étant aussi applicables aux sociétés de financement, aucune modification supplémentaire n'a été nécessaire pour leur appliquer ces nouvelles dispositions.

Le présent article de ce projet de loi vise donc tout d'abord à prendre en compte les modifications en introduisant à l'article L. 511-41-1-B du code monétaire et financier les « politiques et les plans d'urgence et de poursuite de l'activité » ainsi que les « plans de réponse et de rétablissement » à la liste des outils de gestion des risques dont les établissements de crédit doivent disposer. Afin de compléter cette transposition de l'article 4(3) de la directive DORA et d'évoquer spécifiquement les politiques et plans d'urgence et de poursuite de l'activité ainsi que les plans de réponse et de rétablissement spécifiques aux activités de TIC, il est envisagé de modifier également l'article 215 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 soumises au contrôle de l'Autorité de contrôle prudentiel et de résolution.

En outre, le risque lié aux TIC n'est inclus aujourd'hui dans la directive CRD que de façon implicite, dans le cadre du risque opérationnel, dans le processus de contrôle et d'évaluation prudentiels (SREP) mené par les autorités de supervision (Autorité de contrôle prudentielle et de résolution – ACPR et Banque centrale européenne – BCE). Dans un souci de clarté juridique et pour veiller à ce que les autorités de supervision du secteur bancaire cernent efficacement le risque lié aux TIC et contrôlent sa gestion par les entités financières conformément au nouveau cadre sur la résilience opérationnelle numérique, le champ d'application du SREP est modifié à l'article 4(4) de la directive DORA pour se référer explicitement aux exigences fixées dans le règlement (UE) 2022/2554 et couvrir en particulier les risques mis en évidence par les résultats des tests de résilience opérationnelle numérique effectués par les entités financières conformément audit règlement.

Le présent article du projet de loi amende donc l'article L. 511-41-1-B du code monétaire et financier afin d'introduire au sein de la liste des risques devant faire l'objet d'une gestion des

risques au sein des établissements de crédit, les risques liés aux technologies de l'information et de la communication y compris ceux liés aux services fournis par des prestataires tiers, objets du règlement DORA, ainsi que les risques mis en évidence par les tests de résilience opérationnelle numérique.

Les modifications mentionnées ci-dessus sont aussi rendues applicables aux sociétés de financement telles que définies au II de l'article L. 511-1 du code monétaire et financiers. Il s'agit d'établissements financiers, autres que des établissements de crédit, qui effectuent à titre de profession habituelle et pour leur propre compte des opérations de crédit dans les conditions et limites définies par leur agrément (elles ne collectent notamment pas de dépôts et fonds remboursables du public). Il y a 144 entreprises qui disposent aujourd'hui de l'agrément de société de financement et 877 sont agréées en tant qu'établissement de crédit. L'article L. 511-41 et suivants du code monétaire et financier ainsi que l'arrêté du 23 décembre 2013 relatif au régime prudentiel des sociétés de financement prévoient aujourd'hui que les sociétés de financement appliquent déjà les exigences prudentielles prévues au titre de la directive CRD et du règlement associé 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 dit « CRR » - à l'exception des dispositions relatives à la liquidité et au levier. L'application aux sociétés de financement d'exigences prudentielles comparables en termes de solidité à celles applicables aux établissements de crédit – et ce depuis l'entrée en application du cadre prudentiel européen en 2013 – permet notamment à ces premières de bénéficier d'un traitement prudentiel plus favorable, les expositions sur ces sociétés de financement pouvant être traitées comme des expositions sur les établissements de crédit au titre de la réglementation européenne[243]. C'est le maintien de cette comparabilité entre établissements de crédit et sociétés de financement qui est notamment recherché.

4. ANALYSE DES IMPACTS DES DISPOSITIONS ENVISAGEES

4.1. IMPACTS JURIDIQUES

4.1.1. Impacts sur l'ordre juridique interne

L'article L. 511-41-1-B du code monétaire et financier est modifié.

4.1.2. Articulation avec le droit international et le droit de l'Union européenne

[243] Cf. article 119 du règlement CRR.

Cet article vise à transposer des dispositions du droit de l'Union européenne dans le droit interne.

La directive CRD n'énonce actuellement que des règles générales de gouvernance interne des établissements de crédit et des dispositions relatives au risque opérationnel définissant, à l'article L. 511-41-1-B du code monétaire et financier, des exigences en matière de plans d'urgence et de poursuite de l'activité qui servent implicitement de base pour traiter les risques liés aux TIC. Afin de traiter explicitement et clairement ces risques, l'article 4(3) de la directive DORA modifie au sein de l'article 85 de la directive CRD les exigences en matière de plans d'urgence et de poursuite de l'activité de manière à inclure également « les politiques et plans d'urgence et de poursuite de l'activité » ainsi que des « plans de réponse et de rétablissement ». L'article du présent projet de loi vise ainsi à transposer les nouvelles dispositions de l'article 85 de la directive CRD, telles qu'amendées par l'article 4(3) la directive DORA, au sein de l'article L. 511-41-1-B du code monétaire et financier.

4.2. IMPACTS ECONOMIQUES ET FINANCIERS

4.2.1. Impacts macroéconomiques

Sans objet.

4.2.2. Impacts sur les entreprises

Les établissements de crédit ainsi que les sociétés de financement vont devoir appliquer les nouvelles obligations prévues par le règlement DORA et la directive l'accompagnant en matière de résilience opérationnelle numérique. Cela aura un impact en termes financiers, sur les effectifs et sur l'organisation interne de chaque organisme en fonction de sa taille et de son activité. Aujourd'hui, 877 établissements de crédit et 144 sociétés de financement disposent d'un agrément en France[244].

Ces coûts sont toutefois difficiles à quantifier au regard de l'état et du niveau de maturité variable des systèmes informatiques de chaque entreprise. En l'absence d'intervention réglementaire, certaines entreprises financières ont déjà réalisé des investissements importants dans les systèmes informatiques. Cela signifie que, pour les grandes entreprises financières, la mise en œuvre des mesures de cette proposition sera probablement peu coûteuse. Pour les petites entreprises, les coûts devraient également être assez peu élevés, car celles-ci seraient soumises à des mesures moins strictes du fait du risque plus faible qu'elles présentent[245].

[244] Source : Registre des agents financiers – REGAFI.

[245] Voir la publication de la Commission européenne du 24 septembre 2020 : « résumé du rapport d'analyse d'impact accompagnant le document : Proposition de règlement du Parlement européen et du Conseil sur la

4.2.3. Impacts budgétaires

Sans objet.

4.3. IMPACTS SUR LES COLLECTIVITES TERRITORIALES

Sans objet.

4.4. IMPACTS SUR LES SERVICES ADMINISTRATIFS

L'entrée en vigueur de ces nouvelles obligations en matière de cyber-résilience dans le secteur financier va avoir des répercussions sur l'activité de l'Autorité de contrôle prudentiel et de résolution (ACPR) et sur ses besoins en termes de ressources budgétaires et d'effectifs.

A terme, cette règlementation va (i) engendrer de nouvelles missions de surveillance des prestataires tiers de services liés aux TIC et (ii) renforcer les tâches de surveillance sur les assujettis habituels (collecte de nouvelles données, production de nouveaux rapports, etc.). A ce stade, l'ACPR estime qu'une dizaine d'ETP supplémentaires pourrait être nécessaire pour exercer correctement son rôle d'autorité de contrôle dans le cadre de DORA.

4.5. IMPACTS SOCIAUX

4.5.1. Impacts sur la société

Ces nouvelles dispositions permettraient de renforcer le traitement des risques liés aux TIC dans l'ensemble du secteur financier en renforçant les capacités des entités financières à surmonter les incidents informatiques et opérationnels. Cela réduirait le risque de contagion dans l'hypothèse où un cyber-incident se propagerait rapidement au sein des différents acteurs du secteur financier et limiterait ainsi l'impact en termes de stabilité financière. La mise en place d'un ensemble cohérent de règles sur la gestion des risques liés aux tiers prestataires de services informatiques permettrait aux entités financières de mieux contrôler la mesure dans laquelle les tiers prestataires se conforment au cadre réglementaire[246].

4.5.2. Impacts sur les personnes en situation de handicap

résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) nº 1060/2009, (UE) nº 648/2012, (UE) nº 600/2014 et (UE) nº 909/2014 ».

[246] Voir la publication de la Commission européenne du 24 septembre 2020 : « résumé du rapport d'analyse d'impact accompagnant le document : Proposition de règlement du Parlement européen et du Conseil sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) nº 1060/2009, (UE) nº 648/2012, (UE) nº 600/2014 et (UE) nº 909/2014 ».

Sans objet.

4.5.3. Impacts sur l'égalité entre les femmes et les hommes

Sans objet.

4.5.4. Impacts sur la jeunesse

Sans objet.

4.5.5. Impacts sur les professions réglementées

Sans objet.

4.6. IMPACTS SUR LES PARTICULIERS

Ces nouvelles dispositions favoriseraient un environnement opérationnel plus résilient pour les utilisateurs des services offerts par les acteurs du secteur financier. Les consommateurs et des investisseurs bénéficieraient d'une protection renforcée à l'égard des préjudices liés aux incidents informatiques, cyber et opérationnels survenant au sein des secteurs financiers et numériques.

4.7. IMPACTS ENVIRONNEMENTAUX

Sans objet.

5. CONSULTATIONS ET MODALITES D'APPLICATION

5.1. CONSULTATIONS MENEES

En application de l'article L. 614-2 du code monétaire et financier, le Comité consultatif de la législation et de la réglementation financières (CCLRF) a été consulté a rendu un avis favorable le 23 mai 2024.

La rédaction proposée a en outre été envoyée pour information et sur base informelle aux services de l'Autorité de contrôle prudentiel et de résolution (ACPR) et à l'Association française des Sociétés Financières (ASF).

5.2. MODALITES D'APPLICATION

5.2.1. Application dans le temps

Les dispositions du titre III du présent projet de loi entrent en vigueur à compter du 17 janvier 2025.

Toutefois, afin d'accorder un délai de mise en œuvre supplémentaire pour les sociétés de financement considérées comme de taille petite et non-complexes et dont les moyens et ressources sont réputées moins importantes, l'article 62 du projet de loi introduit une entrée en application différée – repoussée d'un an au 17 janvier 2026 – du présent article pour les sociétés de financement remplissant les conditions prévues au point 145 du paragraphe 1 de l'article 4 du règlement (UE) n° 575/2013 du Parlement européen et du Conseil dit « CRR » qui définit les établissements de petite taille et non complexe.

Pour rappel, un établissement de petite taille et non complexe est un établissement qui remplit toutes les conditions suivantes :

a) il ne s'agit pas d'un établissement de grande taille ;

b) la valeur totale de ses actifs sur base individuelle ou, le cas échéant, sur base consolidée conformément au présent règlement et à la directive 2013/36/UE est en moyenne égale ou inférieure à un seuil de cinq milliards d'euros sur la période de quatre ans qui précède immédiatement la période de déclaration annuelle en cours; les États membres peuvent abaisser ce seuil ;

c) 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 conformément à l'article 4 de la directive 2014/59/UE ;

d) son portefeuille de négociation est classé comme étant de faible taille au sens de l'article 94, paragraphe 1 du règlement CRR ;

e) la valeur totale de ses positions sur 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 %, ces deux pourcentages étant calculés conformément à l'article 273 bis, paragraphe 3 ;

f) plus de 75 % du total des actifs et des passifs consolidés de l'établissement, à l'exclusion, dans les deux cas, des expositions intragroupe, sont liés à des activités avec des contreparties situées dans l'Espace économique européen ;

g) l'établissement n'utilise pas de modèles internes pour satisfaire aux exigences prudentielles prévues par le présent règlement, 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 prévues à l'article 433 bis ou 433 quater du règlement CRR sur base consolidée ;

h) 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 ;

i) 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.

Les sociétés de financement remplissant ces conditions sont a priori au nombre de 135. Cette définition d'établissement de petite taille et non complexe s'applique bien aux sociétés de financement puisque les dispositions du règlement européen CRR concerne également cette catégorie d'entité en application de l'article 2 de l'arrêté du 23 novembre 2023 relatif au régime prudentiel des sociétés de financement.

Ainsi, les sociétés de financement ne remplissant pas ces conditions et considérées comme les plus importantes en termes de taille (dont la valeur totale des actifs serait supérieure cinq milliards d'euros, soit une dizaine de sociétés visées) devront appliquer les exigences découlant de la directive et du règlement DORA dès l'entrée en vigueur des dispositions pertinentes de ce projet de loi.

5.2.2. Application dans l'espace

La mesure s'applique à l'ensemble du territoire de la République.

Elle s'applique de plein droit aux collectivités territoriales régies par l'article 73 de la Constitution (Guadeloupe, Guyane, Martinique, La Réunion et Mayotte) et certaines des collectivités relevant de l'article 74 (Saint-Barthélemy, Saint Martin et Saint-Pierre-et-Miquelon).

L'article 4 de la loi du 29 juillet 1961, l'article 7 de la loi organique n° 2004-192 du 27 février 2004 portant statut d'autonomie de la Polynésie Française et l'article 6-2 de la loi n° 99-209 organique du 19 mars 1999 relative à la Nouvelle-Calédonie soumettent respectivement pour les Îles Wallis et Futuna, la Polynésie Française et la Nouvelle-Calédonie au principe de spécialité législative, les lois et règlements n'y étant applicables que sur mention expresse, dès lors qu'ils interviennent dans un domaine pour lequel l'Etat est compétent. En effet, l'Etat est compétent en matière bancaire et financière dans ces collectivités ultramarines régies par le principe de spécialité législative où toute création ou modification du code précité doit être rendue applicable par mention expresse.

Ainsi, l'article 56 du projet de loi rend applicables les présentes dispositions en Nouvelle-Calédonie, en Polynésie française et dans les îles Wallis et Futuna en modifiant les articles L. 773-5, L. 774-5 et L. 775-5 du code monétaire et financier.

Enfin, la modification de l'article L. 712-7 du code monétaire et financier réalisée par l'article 56 du projet de loi rend applicable le règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier à Saint-Pierre et Miquelon, en Nouvelle-Calédonie, en Polynésie française et dans les îles Wallis et Futuna qui sont des pays et territoires d'outre-mer où le droit de l'Union européenne ne s'applique pas.

Par coordination, l'article L. 771-1 est complété par les références au règlement (UE) 2022/2554 précité.

5.2.3. Textes d'application

Le présent article ne requiert aucune mesure d'application.

Article 47 – Référence aux réseaux et systèmes d'information au sein des exigences de contrôle interne des établissements de crédit et des sociétés de financement

1. ÉTAT DES LIEUX

1.1. CADRE GENERAL

L'utilisation généralisée de systèmes de TIC, une numérisation et une connectivité poussées constituent désormais des caractéristiques essentielles des activités des entités financières françaises. A l'aune de ce constat, le règlement européen DORA (UE) 2022/2554 du Parlement européen et du Conseil[247], adopté à l'automne 2022 et entré en vigueur le 16 janvier 2023, renforce les obligations opérationnelles s'imposant aux principaux acteurs du secteur financier. Il est complété par la 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, ci-après « directive DORA » qui regroupe une série de dispositions techniques, visant à clarifier les obligations et à actualiser les références en droit interne de directives.

L'article 74 de la 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, modifiant la directive 2002/87/CE et abrogeant les directives 2006/48/CE et 2006/49/CE (ci-après « CRD ») prévoit notamment que les établissements de crédit, tels que définis au I de l'article L. 511-1 du code monétaire et financier, disposent d'un dispositif solide de gouvernance d'entreprise, comprenant notamment une structure organisationnelle claire avec un partage des responsabilités bien défini, transparent et cohérent, des processus efficaces de détection, de gestion, de suivi et de déclaration des risques auxquels ils sont ou pourraient être exposés, des mécanismes adéquats de contrôle interne, y compris des procédures administratives et comptables saines, et des politiques et pratiques de rémunération permettant et favorisant une gestion saine et efficace des risques.

[247] 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 4(2) de la directive DORA introduit une référence aux réseaux et systèmes d'information[248] mis en place et gérés conformément au règlement DORA comme composante de ce dispositif de gouvernance au sein des établissements de crédit.

Le présent article du projet de loi modifie donc l'article L. 511-55 du code monétaire et financier qui exige que les établissements de crédit et les sociétés de financement se dotent d'un dispositif de gouvernance solide. Le présent article transpose l'article 74 CRD afin d'introduire en droit interne cette référence aux réseaux et systèmes d'information pour les établissements de crédit, mais aussi pour les sociétés de financement, telles que définies au II de l'article L. 511-1 du code monétaire et financier, auxquelles il est prévu qu'elles appliquent les exigences de la directive et du règlement DORA. Il y a aujourd'hui 144 entreprises qui disposent de l'agrément de société de financement et 877 entreprises sont agréées en tant qu'établissement de crédit.

1.2. CADRE CONSTITUTIONNEL

Aux termes de l'article 88-1 de la Constitution : « La République participe aux Communautés européennes et à l'Union européenne, constituées d'Etats qui ont choisi librement, en vertu des traités qui les ont instituées, d'exercer en commun certaines de leurs compétences ». Le Conseil constitutionnel déduit de cette disposition que : « la transposition en droit interne d'une directive communautaire résulte d'une exigence constitutionnelle »[249]. Il en va de même pour une loi ayant pour objet d'adapter le droit interne à un règlement de l'Union européenne[250].

En tout état de cause, la mesure relève du domaine de la loi en application de l'article 34 de la Constitution, au titre des obligations civiles et commerciales.

1.3. CADRE CONVENTIONNEL

Le règlement européen DORA (UE) 2022/2554 du Parlement européen et du Conseil, adopté à l'automne 2022 et entré en vigueur le 16 janvier 2023, renforce les obligations opérationnelles s'imposant aux principaux acteurs du secteur financier. Il est complété par la directive éponyme qui regroupe une série de dispositions techniques, visant à clarifier les

[248] Les réseaux et systèmes d'information sont définis à l'article 6(1) 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. Ceux-ci correspondent notamment à un dispositif interconnecté assurant l'exécution d'un programme ou un traitement automatisé de données numériques.

[249] Voir notamment la décision n° 2004-496 DC du 10 juin 2004, « Loi pour la confiance dans l'économie numérique ».

[250] Voir par exemple la décision n° 2018-765, « Loi relative à la protection des données personnelles », considérant 3.

obligations et à actualiser les références aux enjeux de résilience opérationnelle au sein des directives qui préexistaient au règlement DORA. L'article 4 de la directive DORA liste les amendements apportés à la directive CRD relative encadrant les activités des établissements de crédit et harmonisant leur surveillance prudentielle.

1.4. ÉLEMENTS DE DROIT COMPARE

Les autres Etats membres de l'Union européenne modifieront également leur droit national conformément à la directive DORA afin d'introduire une référence aux réseaux et systèmes d'information au sein des exigences de contrôle interne des établissements de crédit.

2. NECESSITE DE LEGIFERER ET OBJECTIFS POURSUIVIS

2.1. NECESSITE DE LEGIFERER

La nécessité de légiférer provient ici tout d'abord de l'obligation constitutionnelle de transposition en droit interne d'une directive imposée par l'article 88-1 de la Constitution qui dispose que « [l]a République participe à l'Union européenne ». Cette obligation a d'ailleurs été rappelée par le Conseil constitutionnel dans le considérant 7 de sa décision n° 2004-496 DC du 10 juin 2004 : « Considérant qu'aux termes de l'article 88-1 de la Constitution […] ; qu'ainsi, la transposition en droit interne d'une directive communautaire résulte d'une exigence constitutionnelle à laquelle il ne pourrait être fait obstacle qu'en raison d'une disposition expresse contraire de la Constitution ».

Au vu du caractère central de l'utilisation des TIC dans la fourniture de services financiers (à l'instar des réseaux, des infrastructures numériques, des actifs logiciels ou des dispositifs de sauvegarde) et son importance cruciale dans l'exécution des fonctions quotidiennes typiques des entités financières, l'application de ces dispositions permettant la mise en œuvre d'un cadre robuste de résilience opérationnelle numérique est étendue aux sociétés de financement. Cette application des exigences de la directive et du règlement DORA aux sociétés de financement permet en outre de préserver la comparabilité en termes de solidité des régimes applicables respectivement aux établissements de crédit et aux sociétés de financement, condition prévue à l'article 119(5) du règlement 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 dit « CRR » nécessaire au maintien d'un traitement prudentiel plus favorable pour les expositions sur les sociétés de financement. Sans cette comparabilité des exigences, les expositions des établissements de crédit auprès des sociétés de financement auraient dû faire l'objet d'une pondération plus pénalisante application des règles de calcul des exigences de fonds propres au titre du risque de crédit établies par le règlement CRR.

2.2. OBJECTIFS POURSUIVIS

Cet article vise à transposer dans le code monétaire et financier les dispositions des articles 4(2) de la directive DORA, qui modifie les dispositions de l'article 74(1) de la directive CRD relatives au dispositif de gouvernance interne au sein des établissements de crédit. Il étend également ces exigences aux sociétés de financement.

3. OPTIONS POSSIBLES ET DISPOSITIF RETENU

3.1. OPTIONS ENVISAGEES

Suivant le principe du parallélisme des formes, une disposition législative ne peut être modifiée que par une mesure de même niveau normatif. Ainsi, aucune autre option que le recours à la loi n'a été envisagée ici.

3.2. OPTION RETENUE

La directive DORA ne prévoit que des modifications d'ordre technique des différentes directives sectorielles qui visent à assurer la cohérence avec les nouvelles exigences introduites par le règlement DORA. Dans un souci de simplicité et dans la mesure où la transposition de cette directive DORA est sans enjeu majeur, il a été décidé d'introduire les modifications qu'elle prévoit dans les dispositions de droit interne transposant la directive sectorielle CRD applicable aux établissements de crédit (article L. 511-55 du code monétaire et financier). Ces dispositions de droit interne étant également applicables aux sociétés de financement, aucune modification supplémentaire n'a été nécessaire pour leur appliquer ces nouvelles dispositions européennes.

4. ANALYSE DES IMPACTS DES DISPOSITIONS ENVISAGEES

4.1. IMPACTS JURIDIQUES

4.1.1. Impacts sur l'ordre juridique interne

L'article L. 511-55 du code monétaire et financier est modifié.

4.1.2. Articulation avec le droit international et le droit de l'Union européenne

Cet article vise à transposer des dispositions du droit de l'Union européenne dans le droit interne.

L'article 74 de la directive CRD prévoit que les établissements de crédit disposent d'un dispositif de gouvernance solide. L'article 4(2) de la directive DORA introduit une référence aux réseaux et systèmes d'information mis en place et gérés conformément au règlement DORA comme composante de ce dispositif de gouvernance au sein des établissements de crédit. Le présent article modifie donc l'article L. 511-55 du code monétaire et financier qui exige que les établissements de crédit et les sociétés de financement se dotent d'un dispositif de gouvernance solide. Il vise ainsi à transposer les nouvelles dispositions de l'article 74 de la directive CRD, telles qu'amendées par l'article 4(2) de la directive DORA, au sein de l'article L. 511-55 du code monétaire et financier.

4.2. IMPACTS ECONOMIQUES ET FINANCIERS

4.2.1. Impacts macroéconomiques

Sans objet.

4.2.2. Impacts sur les entreprises

Les établissements de crédit ainsi que les sociétés de financement devront s'assurer que leurs réseaux et systèmes d'information sont mis en place et gérés conformément aux exigences du règlement DORA. Cela aura un impact en termes financiers, sur les effectifs et sur l'organisation interne de chaque organisme en fonction de sa taille et de son activité. Aujourd'hui, 877 établissements de crédit et 144 sociétés de financement disposent d'un agrément en France[251]. Ces coûts sont toutefois difficiles à quantifier au regard de l'état et du niveau de maturité variable des systèmes informatiques de chaque entreprise. En l'absence d'intervention réglementaire, certaines entreprises financières ont déjà réalisé des investissements importants dans les systèmes informatiques. Cela signifie que, pour les grandes entreprises financières, la mise en œuvre des mesures de cette proposition sera probablement peu coûteuse. Pour les petites entreprises, les coûts devraient également être assez peu élevés, car celles-ci seraient soumises à des mesures moins strictes du fait du risque plus faible qu'elles présentent[252].

4.2.3. Impacts budgétaires

4.3. IMPACTS SUR LES COLLECTIVITES TERRITORIALES

[251] Source : Registre des agents financiers – REGAFI.

[252] Voir la publication de la Commission européenne du 24 septembre 2020 : « résumé du rapport d'analyse d'impact accompagnant le document : Proposition de règlement du Parlement européen et du Conseil sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) nº 1060/2009, (UE) nº 648/2012, (UE) nº 600/2014 et (UE) nº 909/2014 ».

Sans objet.

4.4. IMPACTS SUR LES SERVICES ADMINISTRATIFS

L'entrée en vigueur de ces nouvelles obligations en matière de cyber-résilience dans le secteur financier va avoir des répercussions sur l'activité de l'Autorité de contrôle prudentiel et de résolution (ACPR) et sur ses besoins en termes de ressources budgétaires et d'effectifs.

A terme, cette règlementation va (i) engendrer de nouvelles missions de surveillance des prestataires tiers de services liés aux TIC et (ii) renforcer les tâches de surveillance sur les assujettis habituels (collecte de nouvelles données, production de nouveaux rapports, etc.). A ce stade, l'ACPR estime qu'une dizaine d'ETP supplémentaires pourrait être nécessaire pour exercer correctement son rôle d'autorité de contrôle dans le cadre de DORA.

4.5. IMPACTS SOCIAUX

4.5.1. Impacts sur la société

Ces nouvelles dispositions permettraient de renforcer le traitement des risques liés aux TIC dans l'ensemble du secteur financier en renforçant les capacités des entités financières à surmonter les incidents informatiques et opérationnels. Cela réduirait le risque de contagion dans l'hypothèse où un cyber-incident se propagerait rapidement au sein des différents acteurs du secteur financier et limiterait ainsi l'impact en termes de stabilité financière. La mise en place d'un ensemble cohérent de règles sur la gestion des risques liés aux tiers prestataires de services informatiques permettrait aux entités financières de mieux contrôler la mesure dans laquelle les tiers prestataires se conforment au cadre réglementaire[253].

4.5.2. Impacts sur les personnes en situation de handicap

Sans objet.

4.5.3. Impacts sur l'égalité entre les femmes et les hommes

Sans objet.

[253] Voir la publication de la Commission européenne du 24 septembre 2020 : « résumé du rapport d'analyse d'impact accompagnant le document : Proposition de règlement du Parlement européen et du Conseil sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) nº 1060/2009, (UE) nº 648/2012, (UE) nº 600/2014 et (UE) nº 909/2014 ».

4.5.4. Impacts sur la jeunesse

Sans objet.

4.5.5. Impacts sur les professions réglementées

Sans objet.

4.6. IMPACTS SUR LES PARTICULIERS

Ces nouvelles dispositions favoriseraient un environnement opérationnel plus résilient pour les utilisateurs des services offerts par les acteurs du secteur financier. Les consommateurs et des investisseurs bénéficieraient d'une protection renforcée à l'égard des préjudices liés aux incidents informatiques, cyber et opérationnels survenant au sein des secteurs financiers et numériques.

4.7. IMPACTS ENVIRONNEMENTAUX

Sans objet.

5. CONSULTATIONS ET MODALITES D'APPLICATION

5.1. CONSULTATIONS MENEES

En application de l'article L. 614-2 du code monétaire et financier, le Comité consultatif de la législation et de la réglementation financières (CCLRF) a été consulté a rendu un avis favorable le 23 mai 2024.

La rédaction proposée a en outre été soumise pour information et sur base informelle aux services de l'Autorité de contrôle prudentiel et de résolution (ACPR) et à l'Association française des Sociétés Financières (ASF).

5.2. MODALITES D'APPLICATION

5.2.1. Application dans le temps

Les dispositions du titre III du présent projet de loi entrent en vigueur à compter du 17 janvier 2025.

Toutefois, afin d'accorder un délai de mise en œuvre supplémentaire pour les sociétés de financement considérées comme de taille petite et non-complexes et dont les moyens et ressources sont réputées moins importantes, l'article 62 du projet de loi introduit une entrée en application différée – repoussée d'un an au 17 janvier 2026 – du présent article pour les sociétés de financement remplissant les conditions prévues au point 145 du paragraphe 1 de l'article 4 du règlement (UE) n° 575/2013 du Parlement européen et du Conseil dit « CRR » qui définit les établissements de petite taille et non complexe.

Pour rappel, un établissement de petite taille et non complexe est un établissement qui remplit toutes les conditions suivantes :

a) il ne s'agit pas d'un établissement de grande taille ;

b) la valeur totale de ses actifs sur base individuelle ou, le cas échéant, sur base consolidée conformément au présent règlement et à la directive 2013/36/UE est en moyenne égale ou inférieure à un seuil de cinq milliards d'euros sur la période de quatre ans qui précède immédiatement la période de déclaration annuelle en cours; les États membres peuvent abaisser ce seuil ;

c) 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 conformément à l'article 4 de la directive 2014/59/UE ;

d) son portefeuille de négociation est classé comme étant de faible taille au sens de l'article 94, paragraphe 1 du règlement CRR ;

e) la valeur totale de ses positions sur 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 %, ces deux pourcentages étant calculés conformément à l'article 273 bis, paragraphe 3 ;

f) plus de 75 % du total des actifs et des passifs consolidés de l'établissement, à l'exclusion, dans les deux cas, des expositions intragroupe, sont liés à des activités avec des contreparties situées dans l'Espace économique européen ;

g) l'établissement n'utilise pas de modèles internes pour satisfaire aux exigences prudentielles prévues par le présent règlement, 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 prévues à l'article 433 bis ou 433 quater du règlement CRR sur base consolidée ;

h) 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 ;

i) 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.

Les sociétés de financement remplissant ces conditions sont a priori au nombre de 135. Cette définition d'établissement de petite taille et non complexe s'applique bien aux sociétés de financement puisque les dispositions du règlement européen CRR concerne également cette catégorie d'entité en application de l'article 2 de l'arrêté du 23 novembre 2023 relatif au régime prudentiel des sociétés de financement.

Ainsi, les sociétés de financement ne remplissant pas ces conditions et considérées comme les plus importantes en termes de taille (dont la valeur totale des actifs serait supérieure cinq milliards d'euros, soit une dizaine de sociétés visées) devront appliquer les exigences découlant de la directive et du règlement DORA dès l'entrée en vigueur des dispositions pertinentes de ce projet de loi.

5.2.2. Application dans l'espace

La mesure s'applique à l'ensemble du territoire de la République.

Elle s'applique de plein droit aux collectivités territoriales régies par l'article 73 de la Constitution (Guadeloupe, Guyane, Martinique, La Réunion et Mayotte) et certaines des collectivités relevant de l'article 74 (Saint-Barthélemy, Saint Martin et Saint-Pierre-et-Miquelon).

L'article 4 de la loi du 29 juillet 1961, l'article 7 de la loi organique n° 2004-192 du 27 février 2004 portant statut d'autonomie de la Polynésie Française et l'article 6-2 de la loi n° 99-209 organique du 19 mars 1999 relative à la Nouvelle-Calédonie soumettent respectivement pour les Îles Wallis et Futuna, la Polynésie Française et la Nouvelle-Calédonie au principe de spécialité législative, les lois et règlements n'y étant applicables que sur mention expresse, dès lors qu'ils interviennent dans un domaine pour lequel l'Etat est compétent. En effet, l'Etat est compétent en matière bancaire et financière dans ces collectivités ultramarines régies par le principe de spécialité législative où toute création ou modification du code précité doit être rendue applicable par mention expresse.

Ainsi, l'article 56 du projet de loi rend applicables les présentes dispositions en Nouvelle-Calédonie, en Polynésie française et dans les îles Wallis et Futuna en modifiant les articles L. 773-6, L. 774-6 et L. 775-6 du code monétaire et financier.

Enfin, la modification de l'article L. 712-7 du code monétaire et financier réalisée par l'article 56 du projet de loi rend applicable le règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier à Saint-Pierre et Miquelon, en Nouvelle-Calédonie, en Polynésie française et dans les îles

Wallis et Futuna qui sont des pays et territoires d'outre-mer où le droit de l'Union européenne ne s'applique pas.

Par coordination, l'article L. 771-1 est complété par les références au règlement (UE) 2022/2554 précité.

5.2.3. Textes d'application

Le présent article ne requiert aucune mesure d'application.

Article 48 - Obligations des prestataires de services de paiement en matière de gestion du risque lié aux technologies de l'information et des communications (TIC)

1. ÉTAT DES LIEUX

1.1. CADRE GENERAL

L'article 95 de la directive (UE) 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015 concernant les services de paiement dans le marché intérieur[254], ci-après « DSP2 », prévoit que les prestataires de services de paiement définis à l'article 1er de la directive[255] établissent un cadre prévoyant des mesures d'atténuation et des mécanismes de contrôle appropriés en vue de gérer les risques opérationnels et de sécurité liés aux services de paiement qu'ils fournissent.

Les prestataires de services de paiement recouvrent notamment :

- les prestataires de services de paiement visés à l'article 1er, paragraphe 1, points a), b) et d), de la DSP2 (à savoir les prestataires de services de paiement au sens du I de l'article L. 521-1 du code monétaire et financier, à savoir les établissements de crédit, les établissements de paiement, les établissements de monnaie électronique) ;
- les prestataires de services d'information sur les comptes, également visés au I de l'article L. 521-1 du code monétaire et financier ;
- les établissements de paiement exemptés en vertu de l'article 32, paragraphe 1, de la DSP2 (à savoir ceux visés à l'article L. 522-11-1 du code monétaire et financier, qui bénéficient d'un agrément simplifié mais qui constituent bien des établissements de paiement à part entière au sens du I de l'article L. 521-1 du code monétaire et financier) ;
- les établissements de monnaie électronique bénéficiant d'une exemption visés à l'article 9, paragraphe 1, de la directive n° 2009/110/CE (à savoir ceux visés à l'article L. 526-19 du code monétaire et financier, qui bénéficient d'un agrément simplifié

[254] 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.

[255] A savoir les établissements de crédit, les établissements de monnaie électronique, les offices de chèques postaux habilités en droit national à fournir des services de paiement, les établissements de paiement, la BCE et les banques centrales nationales lorsqu'elles n'agissent pas en qualité d'autorités monétaires ou d'autres autorités publiques, les Etats membres ou leurs autorités régionales ou locales lorsqu'ils n'agissent pas en qualité d'autorités publiques.

mais qui constituent également des établissements de monnaie électronique au sens du I de l'article L. 521-1 du code monétaire et financier).

Ce cadre doit prévoir que les prestataires de services de paiement établissent et maintiennent des procédures efficaces de gestion des incidents, y compris pour la détection et la classification des incidents opérationnels et de sécurité majeurs.

Ces procédures de gestion des incidents, intégrées aux procédures globales de gestion des risques des prestataires de services de paiement, doivent permettre à l'établissement concerné d'identifier, de mesurer, de suivre et de gérer l'ensemble des risques résultant des activités liées au paiement du prestataire de services de paiement et auxquels est exposé ce prestataire, notamment en matière de continuité des activités.

Elles comprennent notamment le document relatif à la politique de sécurité, et doivent définir et attribuer les principaux rôles et responsabilités, ainsi que le système de déclaration pertinents nécessaires pour faire appliquer les mesures de sécurité et pour gérer les risques opérationnels et de sécurité.

Cet article est transposé à l'article L. 521-9 du code monétaire et financier, qui prévoit l'obligation pour les prestataires de services de paiement de mettre en place des mesures d'atténuation et des mécanismes de contrôle appropriés en vue de gérer les risques opérationnels et de sécurité liés aux services de paiement qu'ils fournissent.

1.2. CADRE CONSTITUTIONNEL

Aux termes de l'article 88-1 de la Constitution : « La République participe aux Communautés européennes et à l'Union européenne, constituées d'Etats qui ont choisi librement, en vertu des traités qui les ont instituées, d'exercer en commun certaines de leurs compétences ». Le Conseil constitutionnel déduit de cette disposition que : « la transposition en droit interne d'une directive communautaire résulte d'une exigence constitutionnelle »[256]. Il en va de même pour une loi ayant pour objet d'adapter le droit interne à un règlement de l'Union européenne[257].

1.3. CADRE CONVENTIONNEL

[256] Voir notamment la décision n° 2004-496 DC du 10 juin 2004, « Loi pour la confiance dans l'économie numérique ».

[257] Voir par exemple la décision n° 2018-765, « Loi relative à la protection des données personnelles », considérant 3.

La directive (UE) 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015 concernant les services de paiement dans le marché intérieur (« DSP2 ») régit la fourniture de services de paiement à des utilisateurs. La fourniture de tels services requiert un agrément en tant que prestataire de services de paiement (en tant qu'établissement de crédit, d'établissement de paiement ou d'établissement de monnaie électronique), sauf exemptions prévues par la directive.

L'article 95 de la DSP2 prévoit que les prestataires de services de paiement établissent un cadre prévoyant des mesures d'atténuation et des mécanismes de contrôle appropriés en vue de gérer les risques opérationnels et de sécurité liés aux services de paiement qu'ils fournissent.

Le 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, ci-après « règlement DORA », établit des exigences uniformes en matière de sécurité des réseaux et des systèmes d'information des entités financières, afin de leur permettre de résister, de répondre et de se remettre de toute perturbation ou menace impliquant les technologies de l'information et de la communication (TIC).

Ce règlement prévoit, de manière harmonisée, que les entités financières doivent déclarer aux autorités compétentes les incidents majeurs qui les affectent en matière de cybersécurité et de paiements.

Dans ce contexte, l'article 7 (4) de la 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, ci-après « directive DORA », vise à éviter un doublon en matière d'exigences liées à la cyber-résilience en modifiant les directives sectorielles qui régissent plusieurs secteurs financiers, dont la fourniture de services de paiement.

L'article 7 (5) de la directive DORA modifie l'article 95 de la DSP2 afin de prévoir que son premier alinéa est « sans préjudice de l'application du chapitre II du règlement (UE) 2022/2554 » aux prestataires de services de paiement.

1.4. ÉLEMENTS DE DROIT COMPARE

Les autres Etats membres de l'Union européenne devront prévoir que leurs prestataires de services de paiement qui constituent également des entités financières devront se conformer aux obligations prévues au chapitre II du règlement DORA.

2. NECESSITE DE LEGIFERER ET OBJECTIFS POURSUIVIS

2.1. NECESSITE DE LEGIFERER

La nécessité de légiférer provient ici de l'obligation constitutionnelle de transposition en droit interne d'une directive imposée par l'article 88-1 de la Constitution qui dispose que « [l]a République participe à l'Union européenne ». Cette obligation a d'ailleurs été rappelée par le Conseil constitutionnel dans le considérant 7 de sa décision n° 2004-496 DC du 10 juin 2004 : « Considérant qu'aux termes de l'article 88-1 de la Constitution […] ; qu'ainsi, la transposition en droit interne d'une directive communautaire résulte d'une exigence constitutionnelle à laquelle il ne pourrait être fait obstacle qu'en raison d'une disposition expresse contraire de la Constitution ».

2.2. OBJECTIFS POURSUIVIS

Cet article permet de transposer dans le code monétaire et financier l'article 7 (4) de la directive DORA, qui prévoit l'articulation du chapitre II du règlement DORA avec l'obligation générale de mise en place d'un cadre prévoyant des mesures d'atténuation et des mécanismes de contrôle appropriés en vue de gérer les risques opérationnels et de sécurité liés aux services de paiement qu'ils fournissent, qui incombe aux prestataires de services de paiement et qui est rappelée à l'article 95 (1) de la DSP2.

3. OPTIONS POSSIBLES ET DISPOSITIF RETENU

3.1. OPTIONS ENVISAGEES

Aucune autre option n'a été envisagée dans la mesure où cette disposition est commandée par une norme supérieure issue du droit de l'Union européenne.

3.2. OPTION RETENUE

La directive DORA ne prévoit que des modifications d'ordre technique des différentes directives sectorielles qui visent à assurer la cohérence avec les nouvelles exigences introduites par le règlement DORA. Dans un souci de simplicité, il a été décidé de modifier l'article L. 521-9 du code monétaire et financier afin de prévoir qu'il s'applique sans préjudice des dispositions, d'application directe, figurant au chapitre II du règlement DORA.

4. ANALYSE DES IMPACTS DES DISPOSITIONS ENVISAGEES

4.1. IMPACTS JURIDIQUES

4.1.1. Impacts sur l'ordre juridique interne

L'article L. 521-9 du code monétaire et financier est modifié.

4.1.2. Articulation avec le droit international et le droit de l'Union européenne

La modification envisagée vise à prendre en compte les modifications apportées par l'article 7 (4) de la directive DORA qui modifie l'article 95 (1) de la directive DSP2 relative à la gestion des risques opérationnels et de sécurité prévoyant les obligations des prestataires de services de paiement.

4.2. IMPACTS ECONOMIQUES ET FINANCIERS

4.2.1. Impacts macroéconomiques

Néant.

4.2.2. Impacts sur les entreprises

Les prestataires de services de paiement qui constituent également des entités financières au sens du règlement DORA devront se conformer aux dispositions du chapitre II du règlement DORA, à savoir les dispositions en matière de gouvernance et d'organisation interne afin de gérer le risque lié aux TIC, aux systèmes, protocoles outils de TIC, à l'identification, à la prévention et à la protection de leurs systèmes et outils TIC. La mise en conformité concerne donc un grand nombre d'acteurs.

L'article 4 du règlement DORA prévoit cependant que les entités financières doivent mettre en œuvre les règles énoncées au chapitre II 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.

4.2.3. Impacts budgétaires

Néant.

4.3. IMPACTS SUR LES COLLECTIVITES TERRITORIALES

Néant. S'agissant d'articles relatifs au droit monétaire, bancaire et financier, le présent article est sans incidence sur le fonctionnement des collectivités territoriales.

4.4. IMPACTS SUR LES SERVICES ADMINISTRATIFS

Néant.

4.5. IMPACTS SOCIAUX

4.5.1. Impacts sur la société

Néant.

4.5.2. Impacts sur les personnes en situation de handicap

Néant.

4.5.3. Impacts sur l'égalité entre les femmes et les hommes

Néant.

4.5.4. Impacts sur la jeunesse

Néant.

4.5.5. Impacts sur les professions réglementées

Néant.

4.6. IMPACTS SUR LES PARTICULIERS

Néant.

4.7. IMPACTS ENVIRONNEMENTAUX

Néant.

5. CONSULTATIONS ET MODALITES D'APPLICATION

5.1. CONSULTATIONS MENEES

En application de l'article L. 614-2 du code monétaire et financier, le Comité consultatif de la législation et de la réglementation financières (CCLRF) a été consulté a rendu un avis favorable le 23 mai 2024.

La rédaction proposée a en outre été envoyée pour information et sur base informelle aux services de l'Autorité de contrôle prudentiel et de résolution (ACPR).

5.2. MODALITES D'APPLICATION

5.2.1. Application dans le temps

Le présent article s'appliquera à compter du 17 janvier 2025 conformément à l'article 62 du présent projet de loi.

5.2.2. Application dans l'espace

La mesure s'applique à l'ensemble du territoire de la République.

Elle s'appliquera de plein droit aux collectivités territoriales régies par l'article 73 de la Constitution (Guadeloupe, Guyane, Martinique, La Réunion et Mayotte) et certaines des collectivités relevant de l'article 74 (Saint-Barthélemy, Saint Martin et Saint-Pierre et Miquelon).

L'article 4 de la loi du 29 juillet 1961, l'article 7 de la loi organique n° 2004-192 du 27 février 2004 portant statut d'autonomie de la Polynésie Française et l'article 6-2 de la loi n° 99-209 organique du 19 mars 1999 relative à la Nouvelle-Calédonie soumettent respectivement pour les Îles Wallis et Futuna, la Polynésie Française et la Nouvelle-Calédonie au principe de spécialité législative, les lois et règlements n'y étant applicables que sur mention expresse, dès lors qu'ils interviennent dans un domaine pour lequel l'Etat est compétent. En effet, l'Etat est compétent en matière bancaire et financière dans ces collectivités ultramarines régies par le principe de spécialité législative où toute création ou modification du code précité doit être rendue applicable par mention expresse.

Ainsi, l'article 56 du projet de loi rend applicables les présentes dispositions en Nouvelle-Calédonie, en Polynésie française et dans les îles Wallis et Futuna en modifiant les articles L. 773-21, L. 774-21 et L. 775-15 du code monétaire et financier.

Enfin, la modification de l'article L. 712-7 du code monétaire et financier réalisée par l'article

47 du projet de loi rend applicable le règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier à Saint-Pierre et Miquelon, en Nouvelle-Calédonie, en Polynésie française et dans les îles Wallis et Futuna qui sont des pays et territoires d'outre-mer où le droit de l'Union européenne ne s'applique pas.

Par coordination, l'article L. 771-1 est complété par les références au règlement (UE) 2022/2554 précité.

5.2.3. Textes d'application

Le présent article ne requiert aucune disposition d'application.

Article 49 – Modification de la liste des prestataires de services de paiement soumis à une obligation de notification des incidents opérationnels ou de sécurité majeur

1. ÉTAT DES LIEUX

1.1. CADRE GENERAL

L'article 96 de la directive (UE) 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015 concernant les services de paiement dans le marché intérieur, ci-après « DSP2 »[258], prévoit qu'en cas d'incident opérationnel ou de sécurité majeur, les prestataires de services de paiement informent sans retard injustifié l'autorité compétente dans l'État membre d'origine du prestataire de services de paiement.

Cet article est transposé à l'article L. 521-10 du code monétaire et financier, selon lequel les prestataires de services de paiement mentionnés à l'article L. 521-1 du code monétaire et financier doivent informer sans retard injustifié l'Autorité de contrôle prudentiel et de résolution (ACPR) de tout incident opérationnel majeur ou la Banque de France en cas d'incident de sécurité majeur.

Lorsque l'incident a ou est susceptible d'avoir des répercussions sur les intérêts financiers de ses utilisateurs de services de paiement, le prestataire de services de paiement informe sans retard injustifié ses utilisateurs de services de paiement de l'incident et de toutes les mesures disponibles qu'ils peuvent prendre pour atténuer les effets dommageables de l'incident.

Dès réception de ces notifications, l'ACPR ou la Banque de France communique sans retard injustifié les détails importants de l'incident à l'Autorité bancaire européenne et à la Banque centrale européenne, et, après avoir évalué la pertinence de l'incident pour d'autres autorités nationales concernées, informe celles-ci en conséquence.

1.2. CADRE CONSTITUTIONNEL

Aux termes de l'article 88-1 de la Constitution : « La République participe aux Communautés européennes et à l'Union européenne, constituées d'Etats qui ont choisi librement, en vertu des traités qui les ont instituées, d'exercer en commun certaines de leurs compétences ». Le Conseil constitutionnel déduit de cette disposition que : « la transposition en droit interne

[258] 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.

d'une directive communautaire résulte d'une exigence constitutionnelle »[259]. Il en va de même pour une loi ayant pour objet d'adapter le droit interne à un règlement de l'Union européenne[260].

1.3. CADRE CONVENTIONNEL

La directive (UE) 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015 concernant les services de paiement dans le marché intérieur (« DSP2 ») régit la fourniture de services de paiement à des utilisateurs. La fourniture de tels services requiert un agrément en tant que prestataire de services de paiement (en tant qu'établissement de crédit, d'établissement de paiement ou d'établissement de monnaie électronique), sauf exemptions prévues par la directive.

L'article 96 de la directive DSP2 prévoit qu'en cas d'incident opérationnel ou de sécurité majeur, les prestataires de services de paiement informent sans retard injustifié l'autorité compétente dans l'État membre d'origine du prestataire de services de paiement.

Le 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, ci-après « règlement DORA », établit des exigences uniformes en matière de sécurité des réseaux et des systèmes d'information des entités financières, afin de leur permettre de résister, de répondre et de se remettre de toute perturbation ou menace impliquant les technologies de l'information et de la communication (TIC).

Dans ce contexte, l'article 7 (5) de la 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, ci-après « directive DORA », vise à éviter un doublonnement en matière de notification aux autorités des incidents opérationnels, en modifiant l'article 96 de la directive (UE) 2015/2366 du 25 novembre 2015 concernant les services de paiement dans le marché intérieur (DSP2)[261], c'est-à-dire, en France, l'Autorité de contrôle prudentiel et de résolution et la Banque de France.

---

[259] Voir notamment la décision n° 2004-496 DC du 10 juin 2004, « Loi pour la confiance dans l'économie numérique ».

[260] Voir par exemple la décision n° 2018-765, « Loi relative à la protection des données personnelles », considérant 3.

[261] Directive (UE) 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015 concernant les services de paiement dans le marché intérieur, modifiant les directives 2002/65/CE, 2009/110/CE et 2013/36/UE et le règlement (UE) n° 1093/2010, et abrogeant la directive 2007/64/CE.

L’article 7 (5) de la directive DORA exclut du champ de l’obligation de notification des incidents les prestataires de services de paiement qui constituent également des entités financières dans le champ du règlement DORA, à savoir les établissements de crédit, les établissements de monnaie électronique et les établissements de paiement, respectivement mentionnés aux points a), b) et d) de l’article 1er de la DSP2.

Les prestataires de services de paiement qui ne constituent pas des entités financières au sens du règlement DORA, à savoir les prestataires de services de paiement mentionnés au II de l’article L. 521-10 du code monétaire et financier (Banque de France, Institut d'émission des départements d'outre-mer, Institut d'émission d'outre-mer, Trésor public, Caisse des dépôts et consignations) restent dans le champ de l’obligation de notification des incidents opérationnels prévu par la DSP2.

1.4. ÉLEMENTS DE DROIT COMPARE

Les autres Etats membres pourront soit décider de maintenir les prestataires de services de paiement qui ne constituent pas des entités financières dans le champ des règles prévues actuellement par la DSP2, soit leur inclure unilatéralement dans le champ du règlement DORA.

2. NECESSITE DE LEGIFERER ET OBJECTIFS POURSUIVIS

2.1. NECESSITE DE LEGIFERER

La nécessité de légiférer provient ici de l’obligation constitutionnelle de transposition en droit interne d’une directive imposée par l’article 88-1 de la Constitution qui dispose que « [l]a République participe à l’Union européenne ». Cette obligation a d’ailleurs été rappelée par le Conseil constitutionnel dans le considérant 7 de sa décision n° 2004-496 DC du 10 juin 2004 : « Considérant qu’aux termes de l’article 88-1 de la Constitution […] ; qu’ainsi, la transposition en droit interne d’une directive communautaire résulte d’une exigence constitutionnelle à laquelle il ne pourrait être fait obstacle qu’en raison d’une disposition expresse contraire de la Constitution ».

2.2. OBJECTIFS POURSUIVIS

Cet article permet de transposer dans le code monétaire et financier l’article 7 (5) de la directive DORA, qui exclut du champ de l’obligation de notification des incidents opérationnels les prestataires de services de paiement qui ne constituent pas des entités financières au sens du règlement DORA, à savoir la Banque de France, l’Institut d'émission

des départements d'outre-mer, l'Institut d'émission d'outre-mer, le Trésor public, ainsi que la Caisse des dépôts et consignations.

L'objectif est ainsi de rationaliser le champ d'application de la procédure de notification des incidents opérationnels ou de sécurité majeurs aux seuls prestataires de services de paiement qui ne seront pas dans le champ du règlement DORA.

3. OPTIONS POSSIBLES ET DISPOSITIF RETENU

3.1. OPTIONS ENVISAGEES

Aucune autre option n'a été envisagée dans la mesure où cette disposition est commandée par une norme supérieure issue du droit de l'Union européenne.

3.2. OPTION RETENUE

La directive DORA ne prévoit que des modifications d'ordre technique des différentes directives sectorielles qui visent à assurer la cohérence avec les nouvelles exigences introduites par le règlement DORA. Dans un souci de simplicité, il a été décidé de modifier l'article L. 521-10 du code monétaire et financier afin de circonscrire son champ d'application aux prestataires de services de paiement mentionnés au II de l'article L. 521-1 du même code.

4. ANALYSE DES IMPACTS DES DISPOSITIONS ENVISAGEES

4.1. IMPACTS JURIDIQUES

4.1.1. Impacts sur l'ordre juridique interne

L'article L. 521-10 du code monétaire et financier est modifié.

4.1.2. Articulation avec le droit international et le droit de l'Union européenne

La modification envisagée vise à prendre en compte les modifications apportées par l'article 7 (5) de la directive DORA qui modifie l'article 96 de la directive DSP2 relative à la notification des incidents opérationnels ou de sécurité majeur. Puisque la notification des incidents affectant les prestataires de services de paiement régis par la DSP2 sera désormais couverte par le règlement DORA, cette modification vise à maintenir cette procédure de notification pour les seuls prestataires de services de paiement qui ne sont pas dans le champ de la DSP2.

4.2. IMPACTS ECONOMIQUES ET FINANCIERS

4.2.1. Impacts macroéconomiques

Néant.

4.2.2. Impacts sur les entreprises

Néant.

4.2.3. Impacts budgétaires

Néant.

4.3. IMPACTS SUR LES COLLECTIVITES TERRITORIALES

Néant. S'agissant d'articles relatifs au droit monétaire, bancaire et financier, le présent article est sans incidence sur le fonctionnement des collectivités territoriales.

4.4. IMPACTS SUR LES SERVICES ADMINISTRATIFS

Les prestataires de services de paiement qui constituent également des entités financières dans le cadre du règlement DORA ne relèveront plus du champ de l'obligation de notification des incidents.

4.5. IMPACTS SOCIAUX

4.5.1. Impacts sur la société

Néant.

4.5.2. Impacts sur les personnes en situation de handicap

Néant.

4.5.3. Impacts sur l'égalité entre les femmes et les hommes

Néant.

4.5.4. Impacts sur la jeunesse

Néant.

4.5.5. Impacts sur les professions réglementées

Néant.

4.6. IMPACTS SUR LES PARTICULIERS

Néant.

4.7. IMPACTS ENVIRONNEMENTAUX

Néant.

5. CONSULTATIONS ET MODALITES D'APPLICATION

5.1. CONSULTATIONS MENEES

En application de l'article L. 614-2 du code monétaire et financier, le Comité consultatif de la législation et de la réglementation financières (CCLRF) a été consulté a rendu un avis favorable le 23 mai 2024.

La rédaction proposée a en outre été envoyée pour information et sur base informelle aux services de l'Autorité de contrôle prudentiel et de résolution (ACPR).

5.2. MODALITES D'APPLICATION

5.2.1. Application dans le temps

Le présent article s'appliquera à compter du 17 janvier 2025 conformément à l'article 62 du présent projet de loi.

5.2.2. Application dans l'espace

La mesure s'applique à l'ensemble du territoire de la République.

Elle s'applique de plein droit aux collectivités territoriales régies par l'article 73 de la Constitution (Guadeloupe, Guyane, Martinique, La Réunion et Mayotte) et certaines des collectivités relevant de l'article 74 (Saint-Barthélemy, Saint Martin et Saint-Pierre-et-Miquelon).

L'article 4 de la loi du 29 juillet 1961, l'article 7 de la loi organique n° 2004-192 du 27 février 2004 portant statut d'autonomie de la Polynésie Française et l'article 6-2 de la loi n° 99-209 organique du 19 mars 1999 relative à la Nouvelle-Calédonie soumettent respectivement pour les Îles Wallis et Futuna, la Polynésie Française et la Nouvelle-Calédonie au principe de spécialité législative, les lois et règlements n'y étant applicables que sur mention expresse, dès lors qu'ils interviennent dans un domaine pour lequel l'Etat est compétent. En effet, l'Etat est compétent en matière bancaire et financière dans ces collectivités ultramarines régies par le principe de spécialité législative où toute création ou modification du code précité doit être rendue applicable par mention expresse.

Ainsi, l'article 56 du projet de loi rend applicables les présentes dispositions en Nouvelle-Calédonie, en Polynésie française et dans les îles Wallis et Futuna en modifiant les articles L. 773-21, L. 774-21 et L. 775-15 du code monétaire et financier.

Enfin, la modification de l'article L. 712-7 du code monétaire et financier réalisée par l'article 47 du projet de loi rend applicable le règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier à Saint-Pierre et Miquelon, en Nouvelle-Calédonie, en Polynésie française et dans les îles Wallis et Futuna qui sont des pays et territoires d'outre-mer où le droit de l'Union européenne ne s'applique pas.

Par coordination, l'article L. 771-1 est complété par les références au règlement (UE) 2022/2554 précité.

5.2.3. Textes d'application

Le présent article ne requiert aucune mesure d'application.

Article 50 – Référence aux réseaux et systèmes d'information au sein des exigences de contrôle et de sauvegarde des prestataires de service d'investissement

1. ÉTAT DES LIEUX

1.1. CADRE GENERAL

L'utilisation généralisée de systèmes de technologies de l'information et de la communication (TIC), une numérisation et une connectivité poussées constituent désormais des caractéristiques essentielles des activités des entités financières françaises. A l'aune de ce constat, le 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, ci-après « règlement DORA », adopté à l'automne 2022 et entré en vigueur le 16 janvier 2023, renforce les obligations opérationnelles s'imposant aux principaux acteurs du secteur financier. Il est complété par la 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, ci-après « directive DORA », qui regroupe une série de dispositions techniques, visant à clairier les obligations et à actualiser les références en droit interne de directives.

L'article 74 de la 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, modifiant la directive 2002/87/CE et abrogeant les directives 2006/48/CE et 2006/49/CE (ci-après « CRD ») prévoit que les établissements tels que définis à l'article 4(1)(3) du règlement CRR, c'est-à-dire à la fois les établissements de crédit et les entreprises d'investissement, disposent d'un dispositif solide de gouvernance d'entreprise, comprenant notamment une structure organisationnelle claire avec un partage des responsabilités bien défini, transparent et cohérent, des processus efficaces de détection, de gestion, de suivi et de déclaration des risques auxquels ils sont ou pourraient être exposés, des mécanismes adéquats de contrôle interne, y compris des procédures administratives et comptables saines, et des politiques et pratiques de rémunération permettant et favorisant une gestion saine et efficace des risques.

L'article 4(2) de la directive DORA introduit une référence aux réseaux et systèmes d'information[262] mis en place et gérés conformément au règlement DORA comme composante de ce dispositif de gouvernance au sein des établissements au sens du règlement CRR.

L'article 47 du projet de loi prévoit déjà de modifier l'article L. 511-55 du code monétaire et financier pour transposer l'article 4(2) de la directive DORA en ce qui concerne les établissements de crédit. En complément, le présent article du projet de loi modifie l'article L. 533-2 du code monétaire et financier qui exige que les entreprises d'investissement correspondant à des prestataires de services d'investissement autres que des sociétés de gestion de portefeuille se dotent d'un dispositif de gouvernance solide. Il transpose l'article 74 CRD afin d'introduire en droit interne une référence aux réseaux et systèmes d'information pour les entreprises d'investissement.

1.2. CADRE CONSTITUTIONNEL

Aux termes de l'article 88-1 de la Constitution : « La République participe aux Communautés européennes et à l'Union européenne, constituées d'Etats qui ont choisi librement, en vertu des traités qui les ont instituées, d'exercer en commun certaines de leurs compétences ». Le Conseil constitutionnel déduit de cette disposition que : « la transposition en droit interne d'une directive communautaire résulte d'une exigence constitutionnelle »[263]. Il en va de même pour une loi ayant pour objet d'adapter le droit interne à un règlement de l'Union européenne[264].

Dans l'hypothèse où le juge constitutionnel examinerait la constitutionnalité de ces dispositions, le présent article n'est en contrariété avec aucune règle ou norme de valeur constitutionnelle.

Par ailleurs, la mesure relève du domaine de la loi en application de l'article 34 de la Constitution, au titre des obligations civiles et commerciales.

1.3. CADRE CONVENTIONNEL

[262] Les réseaux et systèmes d'information sont définis à l'article 6(1) 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. Ceux-ci correspondent notamment à un dispositif interconnecté assurant l'exécution d'un programme ou un traitement automatisé de données numériques.

[263] Voir notamment la décision n° 2004-496 DC du 10 juin 2004, « Loi pour la confiance dans l'économie numérique ».

[264] Voir par exemple la décision n° 2018-765, « Loi relative à la protection des données personnelles », considérant 3.

Le règlement européen DORA (UE) 2022/2554 du Parlement européen et du Conseil, adopté à l'automne 2022 et entré en vigueur le 16 janvier 2023, renforce les obligations opérationnelles s'imposant aux principaux acteurs du secteur financier. Il est complété par la directive éponyme qui regroupe une série de dispositions techniques, visant à clarifier les obligations et à actualiser les références aux enjeux de résilience opérationnelle au sein des directives qui préexistaient au règlement DORA. L'article 4 de la directive DORA liste les amendements apportés à la directive CRD relative encadrant les activités des établissements de crédit et harmonisant leur surveillance prudentielle.

1.4. ÉLEMENTS DE DROIT COMPARE

Les autres Etats membres de l'Union européenne modifieront également leur droit national conformément à la directive DORA afin d'introduire une référence aux réseaux et systèmes d'information au sein des exigences de contrôle et de sauvegarde des prestataires de service d'investissement.

2. NECESSITE DE LEGIFERER ET OBJECTIFS POURSUIVIS

2.1. NECESSITE DE LEGIFERER

Cet article vient actualiser l'article L. 533-2 du code monétaire et financier en introduisant la mention des réseaux et systèmes d'information mis en place et gérés conformément au règlement DORA.

2.2. OBJECTIFS POURSUIVIS

Cet article vise à transposer dans le code monétaire et financier les dispositions des articles 4(2) de la directive DORA, qui modifie les dispositions de l'article 74(1) de la directive CRD concernant notamment le dispositif de gouvernance interne au sein des entreprises d'investissement, en particulier les prestataires de services d'investissement autres que les sociétés de gestion de portefeuille.

3. OPTIONS POSSIBLES ET DISPOSITIF RETENU

3.1. OPTIONS ENVISAGEES

Suivant le principe du parallélisme des formes, une disposition législative ne peut être modifiée que par une mesure de même niveau normatif. Ainsi, aucune autre option que le recours à la loi n'a été envisagée ici.

3.2. OPTION RETENUE

Le présent article du projet de loi modifie l'article L. 533-2 du code monétaire et financier relatif aux dispositions prudentielles applicables aux prestataires de services d'investissement autres que les sociétés de gestion de portefeuille afin de préciser que les dispositifs de contrôle et de sauvegarde des systèmes informatiques au sein de ces entités concernent également les réseaux et systèmes d'information mis en place et gérés conformément au 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, ci-après « règlement DORA ».

4. ANALYSE DES IMPACTS DES DISPOSITIONS ENVISAGEES

4.1. IMPACTS JURIDIQUES

4.1.1. Impacts sur l'ordre juridique interne

L'article L. 533-2 du code monétaire et financier est modifié.

4.1.2. Articulation avec le droit international et le droit de l'Union européenne

La présente disposition introduit les exigences du chapitre II du règlement DORA, notamment son article 5, dans le droit interne.

L'article 74 de la directive CRD prévoit que les établissements de crédit disposent d'un dispositif de gouvernance solide. L'article 4(2) de la directive DORA introduit une référence aux réseaux et systèmes d'information mis en place et gérés conformément au règlement DORA comme composante de ce dispositif de gouvernance au sein des établissements au sens du règlement CRR, couvrant à la fois les établissements de crédit et les entreprises d'investissement.

Le présent article du projet de loi modifie l'article L. 533-2 du code monétaire et financier qui exige que les entreprises d'investissement correspondant aux prestataires de services d'investissement autres que les sociétés de gestion de portefeuille se dotent d'un dispositif de gouvernance solide. Il vise ainsi à transposer les nouvelles dispositions de l'article 74 de la

directive CRD, telles qu'amendées par l'article 4(2) de la directive DORA, au sein de l'article L. 533-2 du code monétaire et financier.

4.2. IMPACTS ECONOMIQUES ET FINANCIERS

4.2.1. Impacts macroéconomiques

Sans objet.

4.2.2. Impacts sur les entreprises

Les prestataires de services d'investissement autres que les sociétés de gestion de portefeuille vont devoir prendre en compte les réseaux et systèmes d'information tels que prévus par le règlement DORA dans leur dispositif de contrôle interne et de sauvegarde. Cela aura un impact en termes financiers, sur les effectifs et sur l'organisation interne de chaque organisme en fonction de sa taille et de son activité. Ces coûts sont toutefois difficiles à quantifier au regard de l'état et du niveau de maturité variable des systèmes informatiques de chaque entreprise. En l'absence d'intervention réglementaire, certaines entreprises financières ont déjà réalisé des investissements importants dans les systèmes informatiques. Cela signifie que, pour les grandes entreprises financières, la mise en œuvre des mesures de cette proposition sera probablement peu coûteuse. Pour les petites entreprises, les coûts devraient également être assez peu élevés, car celles-ci seraient soumises à des mesures moins strictes du fait du risque plus faible qu'elles présentent[265].

4.2.3. Impacts budgétaires

Sans objet.

4.3. IMPACTS SUR LES COLLECTIVITES TERRITORIALES

Sans objet.

4.4. IMPACTS SUR LES SERVICES ADMINISTRATIFS

[265] Voir la publication de la Commission européenne du 24 septembre 2020 : « résumé du rapport d'analyse d'impact accompagnant le document : Proposition de règlement du Parlement européen et du Conseil sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) nº 1060/2009, (UE) nº 648/2012, (UE) nº 600/2014 et (UE) nº 909/2014 ».

Sans objet.

4.5. IMPACTS SOCIAUX

4.5.1. Impacts sur la société

Sans objet.

4.5.2. Impacts sur les personnes en situation de handicap

Sans objet.

4.5.3. Impacts sur l'égalité entre les femmes et les hommes

Sans objet.

4.5.4. Impacts sur la jeunesse

Sans objet.

4.5.5. Impacts sur les professions réglementées

Sans objet.

4.6. IMPACTS SUR LES PARTICULIERS

Sans objet.

4.7. IMPACTS ENVIRONNEMENTAUX

Sans objet.

5. CONSULTATIONS ET MODALITES D'APPLICATION

5.1. CONSULTATIONS MENEES

En application de l'article L. 614-2 du code monétaire et financier, le Comité consultatif de la législation et de la réglementation financières (CCLRF) a été consulté a rendu un avis favorable le 23 mai 2024.

La rédaction proposée a en outre été soumise pour information et sur base informelle aux services de l'Autorité de contrôle prudentiel et de résolution (ACPR) et à l'Association française des Sociétés Financières (ASF).

5.2. MODALITES D'APPLICATION

5.2.1. Application dans le temps

Le présent article s'appliquera à compter du 17 janvier 2025 conformément à l'article 62 du présent projet de loi.

5.2.2. Application dans l'espace

La mesure s'applique à l'ensemble du territoire de la République.

Elle s'applique de plein droit aux collectivités territoriales régies par l'article 73 de la Constitution (Guadeloupe, Guyane, Martinique, La Réunion et Mayotte) et certaines des collectivités relevant de l'article 74 (Saint-Barthélemy, Saint Martin et Saint-Pierre-et-Miquelon).

L'article 4 de la loi du 29 juillet 1961, l'article 7 de la loi organique n° 2004-192 du 27 février 2004 portant statut d'autonomie de la Polynésie Française et l'article 6-2 de la loi n° 99-209 organique du 19 mars 1999 relative à la Nouvelle-Calédonie soumettent respectivement pour les Îles Wallis et Futuna, la Polynésie Française et la Nouvelle-Calédonie au principe de spécialité législative, les lois et règlements n'y étant applicables que sur mention expresse, dès lors qu'ils interviennent dans un domaine pour lequel l'Etat est compétent. En effet, l'Etat est compétent en matière bancaire et financière dans ces collectivités ultramarines régies par le principe de spécialité législative où toute création ou modification du code précité doit être rendue applicable par mention expresse.

Ainsi, l'article 56 du projet de loi rend applicables les présentes dispositions en Nouvelle-Calédonie, en Polynésie française et dans les îles Wallis et Futuna en modifiant les articles L. 773-30, L. 774-30 et L. 775-24 du code monétaire et financier.

Enfin, la modification de l'article L. 712-7 du code monétaire et financier réalisée par l'article 56 du projet de loi rend applicable le règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier à Saint-Pierre et Miquelon, en Nouvelle-Calédonie, en Polynésie française et dans les îles

Wallis et Futuna qui sont des pays et territoires d'outre-mer où le droit de l'Union européenne ne s'applique pas.

Par coordination, l'article L. 771-1 est complété par les références au règlement (UE) 2022/2554 précité.

5.2.3. Textes d'application

Le présent article ne requiert aucune mesure d'application.

Article 51 - Systèmes de technologies de l'information et de la communication (TIC) et dispositifs de contrôle des prestataires de services d'investissement

1. ÉTAT DES LIEUX

1.1. CADRE GENERAL

L'article L. 533-10 du code monétaire et financier définit les règles d'organisation applicables aux prestataires de services d'investissement afin de prévenir les conflits d'intérêts, assurer la continuité et la sécurité des services, sauvegarder les actifs des clients, et maintenir des enregistrements détaillés de leurs activités, y compris les conversations téléphoniques et communications électroniques. Le I. et le II. de l'article L. 533-10 précisent ces obligations notamment en matière de prévention des conflits d'intérêt et de garantie de la continuité de la fourniture de services, portant respectivement sur les sociétés de gestion de portefeuille et les prestataires de services d'investissement autres que les sociétés de gestion de portefeuille. Les sociétés de gestion de portefeuille sont définies à l'article L. 532-9 du code monétaire et financier comme des personnes morales gérant un ou plusieurs fonds d'investissement.

Il est proposé de modifier le I. ainsi que le II. de l'article L. 533-10 du code monétaire et financier afin d'introduire une référence au 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, ci-après « règlement DORA », dans la mise en place des dispositifs de contrôle et de sauvegarde dans le domaine du traitement électronique des données, réseaux et systèmes d'information par les sociétés de gestion de portefeuille, et dans l'usage de systèmes de technologies de l'information et de la communication, devant être mis en place et gérés conformément à l'article 7 du règlement DORA. Ces dispositifs de contrôle doivent comprendre des infrastructures informatiques, des protocoles et des outils de traitement de la donnée adaptés à l'ampleur des volumes traités au quotidien, fiables – ce qui suppose une capacité de traitement des données sûre et proportionnée aux flux, et résilients sur le plan technologique.

1.2. CADRE CONSTITUTIONNEL

Aux termes de l'article 88-1 de la Constitution : « La République participe aux Communautés européennes et à l'Union européenne, constituées d'Etats qui ont choisi librement, en vertu des traités qui les ont instituées, d'exercer en commun certaines de leurs compétences ». Le Conseil constitutionnel déduit de cette disposition que : « la transposition en droit interne

d'une directive communautaire résulte d'une exigence constitutionnelle »[266]. Il en va de même pour une loi ayant pour objet d'adapter le droit interne à un règlement de l'Union européenne[267].

1.3. CADRE CONVENTIONNEL

Le règlement DORA fixe des exigences uniformes en matière de sécurité des réseaux et des systèmes d'informations des entités financières, afin de leur permettre de mettre en place les garanties nécessaires face aux perturbations ou menaces impliquant les technologies de l'information et de la communication (TIC). Il fixe un cadre harmonisé en matière de gestion des risques liés aux TIC qui remplace les cadres existants fixés par les directives sectorielles, y compris, s'agissant des marchés d'instruments financiers, par la 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 (MIFID II) et, s'agissant des organismes de placement collectif en valeurs mobilières (OPCVM), par la directive 2009/65/CE du Parlement européen et du Conseil du 13 juillet 2009 portant coordination des dispositions législatives, réglementaires et administratives concernant certains organismes de placement collectif en valeurs mobilières (OPCVM).

En conséquence, la 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, ci-après « directive DORA », modifie plusieurs directives sectorielles.

L'article 6.1.a) de la directive DORA précise que les ressources et procédures utilisées par les sociétés de gestion de portefeuille afin de garantir la continuité et la régularité de la fourniture des services d'investissement doivent être conformes à l'article 7 du règlement DORA, et l'article 1.1 de la directive DORA précise les procédures administratives et comptables les dispositifs de contrôle et de sauvegarde dans le domaine du traitement électronique des donnée devant être mis en œuvre par les sociétés de gestion de portefeuille à l'article 12 de la directive OPCVM.

1.4. ÉLEMENTS DE DROIT COMPARE

[266] Voir notamment la décision n° 2004-496 DC du 10 juin 2004, « Loi pour la confiance dans l'économie numérique ».

[267] Voir par exemple la décision n° 2018-765, « Loi relative à la protection des données personnelles », considérant 3.

Nous ne disposons pas d'informations s'agissant de la manière dont les autres Etats membres ont transposé cet article.

2. NECESSITE DE LEGIFERER ET OBJECTIFS POURSUIVIS

2.1. NECESSITE DE LEGIFERER

La nécessité de légiférer provient ici de l'obligation constitutionnelle de transposition en droit interne d'une directive imposée par l'article 88-1 de la Constitution qui dispose que « [l]a République participe à l'Union européenne ». Cette obligation a d'ailleurs été rappelée par le Conseil constitutionnel dans le considérant 7 de sa décision n° 2004-496 DC du 10 juin 2004 : « Considérant qu'aux termes de l'article 88-1 de la Constitution […] ; qu'ainsi, la transposition en droit interne d'une directive communautaire résulte d'une exigence constitutionnelle à laquelle il ne pourrait être fait obstacle qu'en raison d'une disposition expresse contraire de la Constitution ».

2.2. OBJECTIFS POURSUIVIS

Le présent article permet de transposer à l'article L. 533-10 du code monétaire et financier relatif aux obligations des prestataires de services d'investissement, les exigences rendues applicables par le règlement DORA dans la mise en place des dispositifs de contrôle et de sauvegarde dans le domaine du traitement électronique des données, réseaux et systèmes d'information.

3. OPTIONS POSSIBLES ET DISPOSITIF RETENU

3.1. OPTIONS ENVISAGEES

Aucune autre option n'a été envisagée dans la mesure où cette disposition est commandée par une norme supérieure issue du droit de l'Union européenne.

3.2. OPTION RETENUE

La directive DORA ne prévoit que des modifications d'ordre technique des différentes directives sectorielles qui visent à assurer la cohérence avec les nouvelles exigences introduites par le règlement DORA. Il a été décidé de modifier l'article L. 533-10 du code monétaire et financier relatif aux obligations des prestataires de services d'investissement en rajoutant dans le titre I le point 6° qui transpose textuellement l'article 6 1) b) de la directive

DORA modifiant la directive MiFID II précitée. De même, le 4° du titre II transpose l'article 6 1) a) de la directive DORA et le 5° du titre II transpose l'article 6)1) b) sur les mécanismes de sécurité solides pour garantir la sécurité et l'authentification des moyens de transfert de l'information.

4. ANALYSE DES IMPACTS DES DISPOSITIONS ENVISAGEES

4.1. IMPACTS JURIDIQUES

4.1.1. Impacts sur l'ordre juridique interne

La présente disposition modifie l'article L. 533-10 du code monétaire et financier.

4.1.2. Articulation avec le droit international et le droit de l'Union européenne

La présente disposition est conforme au droit de l'Union européenne, reprenant la rédaction formulée à l'article 6.1 de la directive DORA.

4.2. IMPACTS ECONOMIQUES ET FINANCIERS

4.2.1. Impacts macroéconomiques

Néant.

4.2.2. Impacts sur les entreprises

Conformément aux exigences de la directive DORA, les sociétés de gestion de portefeuille agréés en France[268] devront mettre en place ou actualiser les mécanismes de contrôle interne et d'évaluation des risques en matière de traitement électronique des données pour assurer la sécurité et l'authentification des moyens de transfert de l'information, réduire le risque d'altération des données et protéger la confidentialité des données. Pour ce faire, elles devront déployer des systèmes de TIC appropriés et proportionnés qui devront être gérés conformément aux exigences rendues applicables par le règlement DORA.

4.2.3. Impacts budgétaires

Néant.

[268] 702 sociétés agréées en France fin 2022.

4.3. IMPACTS SUR LES COLLECTIVITES TERRITORIALES

Néant. S'agissant d'articles relatifs au droit monétaire, bancaire et financier, le présent article est sans incidence sur le fonctionnement des collectivités territoriales.

4.4. IMPACTS SUR LES SERVICES ADMINISTRATIFS

Néant.

4.5. IMPACTS SOCIAUX

4.5.1. Impacts sur la société

Néant.

4.5.2. Impacts sur les personnes en situation de handicap

Néant.

4.5.3. Impacts sur l'égalité entre les femmes et les hommes

Néant.

4.5.4. Impacts sur la jeunesse

Néant.

4.5.5. Impacts sur les professions réglementées

Néant.

4.6. IMPACTS SUR LES PARTICULIERS

Néant.

4.7. IMPACTS ENVIRONNEMENTAUX

Néant.

5. CONSULTATIONS ET MODALITES D'APPLICATION

5.1. CONSULTATIONS MENEES

En application de l'article L. 614-2 du code monétaire et financier, le Comité consultatif de la législation et de la réglementation financières (CCLRF) a été consulté a rendu un avis favorable le 23 mai 2024.

La rédaction proposée a en outre été envoyée pour information et sur base informelle à l'Autorité des marchés financiers, qui a contribué à sa préparation.

5.2. MODALITES D'APPLICATION

5.2.1. Application dans le temps

Le présent article s'appliquera à compter du 17 janvier 2025 conformément à l'article 62 du présent projet de loi.

5.2.2. Application dans l'espace

La mesure s'applique à l'ensemble du territoire de la République.

Elle s'applique de plein droit aux collectivités territoriales régies par l'article 73 de la Constitution (Guadeloupe, Guyane, Martinique, La Réunion et Mayotte) et certaines des collectivités relevant de l'article 74 (Saint-Barthélemy, Saint Martin et Saint-Pierre-et-Miquelon).

L'article 4 de la loi du 29 juillet 1961, l'article 7 de la loi organique n° 2004-192 du 27 février 2004 portant statut d'autonomie de la Polynésie Française et l'article 6-2 de la loi n° 99-209 organique du 19 mars 1999 relative à la Nouvelle-Calédonie soumettent respectivement pour les Îles Wallis et Futuna, la Polynésie Française et la Nouvelle-Calédonie au principe de spécialité législative, les lois et règlements n'y étant applicables que sur mention expresse, dès lors qu'ils interviennent dans un domaine pour lequel l'Etat est compétent. En effet, l'Etat est compétent en matière bancaire et financière dans ces collectivités ultramarines régies par le principe de spécialité législative où toute création ou modification du code précité doit être rendue applicable par mention expresse.

Ainsi, l'article 56 du projet de loi rend applicables les présentes dispositions en Nouvelle-Calédonie, en Polynésie française et dans les îles Wallis et Futuna en modifiant les articles L. 773-30, L. 774-30 et L. 775-24 du code monétaire et financier.

Enfin, la modification de l'article L. 712-7 du code monétaire et financier réalisée par l'article 56 du projet de loi rend applicable le règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier à Saint-Pierre et Miquelon, en Nouvelle-Calédonie, en Polynésie française et dans les îles Wallis et Futuna qui sont des pays et territoires d'outre-mer où le droit de l'Union européenne ne s'applique pas.

Par coordination, l'article L. 771-1 est complété par les références au règlement (UE) 2022/2554 précité.

5.2.3. Textes d'application

Le présent article ne requiert aucune mesure d'application.

Article 52 – Systèmes de contrôle des risques mis en œuvre par les prestataires de services d'investissement autres que les sociétés de gestion de portefeuille qui ont recours à la négociation algorithmique

1. ÉTAT DES LIEUX

1.1. CADRE GENERAL

L'article L. 533-10-4 du code monétaire et financier définit les systèmes et contrôles des risques devant être mis en place par les prestataires de services d'investissement autres que les sociétés de gestion de portefeuille qui ont recours à la négociation algorithmique, et leur impose de disposer de plans de continuité des activités efficaces pour faire face à toute défaillance de leurs systèmes de négociation. Par prestataires de services d'investissement hors société de gestion de portefeuille, on entend les entreprises d'investissement ainsi que les établissements de crédit ayant reçu un agrément par l'AMF leur permettant de fournir les services mentionnés à l'article L. 321-1 du code monétaire et financier : 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.

Il est proposé de modifier cet article afin d'y introduire une référence au chapitre II du règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) n° 1060/2009, (UE) n° 648/2012, (UE) n° 600/2014, (UE) n° 909/2014 et (UE) 2016/1011, ci-après « règlement DORA », dans la définition des objectifs assignés aux systèmes et contrôles des risques mis en œuvre par les entreprise d'investissement recourant au trading algorithmique et d'introduire une obligation de mise en œuvre de politiques et de plans en matière de continuité des activités liées aux technologies de l'information et de la communication (TIC), et de plans de réponse et de rétablissement des technologies de l'information et de la communication.

Le trading algorithmique est une modalité de trading qui consiste à utiliser des plateformes qui automatisent la saisie des ordres de bourse en laissant un algorithme décider des différents paramètres de l'ordre (prix de saisie, volume des positions, instants d'ouverture et de clôture) en autonomie.

1.2. CADRE CONSTITUTIONNEL

Aux termes de l'article 88-1 de la Constitution : « La République participe aux Communautés européennes et à l'Union européenne, constituées d'Etats qui ont choisi librement, en vertu des traités qui les ont instituées, d'exercer en commun certaines de leurs compétences ». Le Conseil constitutionnel déduit de cette disposition que : « la transposition en droit interne d'une directive communautaire résulte d'une exigence constitutionnelle »[269]. Il en va de même pour une loi ayant pour objet d'adapter le droit interne à un règlement de l'Union européenne[270].

1.3. CADRE CONVENTIONNEL

Le règlement DORA précité fixe des exigences uniformes en matière de sécurité des réseaux et des systèmes d'informations des entités financières, afin de leur permettre de mettre en place les garanties nécessaires face aux perturbations ou menaces impliquant les technologies de l'information et de la communication (TIC). Ce règlement fixe un cadre harmonisé en matière de gestion des risques liés aux TIC qui remplace les cadres existants fixés par les directives sectorielles, y compris, s'agissant des marchés d'instruments financiers, par la 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 (MIFID II) et, s'agissant des organismes de placement collectif en valeurs mobilières (OPCVM), par la directive 2009/65/CE du Parlement européen et du Conseil du 13 juillet 2009 portant coordination des dispositions législatives, réglementaires et administratives concernant certains organismes de placement collectif en valeurs mobilières (OPCVM), ci-après « directive OPCM ».

En conséquence, la 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, ci-après « directive DORA », modifie plusieurs directives sectorielles.

L'article 6.2.a) de la directive DORA intègre une référence au règlement DORA dans les exigences relatives aux plans en matière de continuité des activités liées aux technologies de l'information et de la communication dont doivent disposer les entreprises d'investissement recourant au trading algorithmique, à l'article 17 de la directive MiFID II.

1.4. ÉLEMENTS DE DROIT COMPARE

[269] Voir notamment la décision n° 2004-496 DC du 10 juin 2004, « Loi pour la confiance dans l'économie numérique ».

[270] Voir par exemple la décision n° 2018-765, « Loi relative à la protection des données personnelles », considérant 3.

Les autres Etats membres devront également transposer cette directive en droit national. Nous ne disposons pas d'informations s'agissant de la manière dont les autres Etats membres transposeront cet article.

2. NECESSITE DE LEGIFERER ET OBJECTIFS POURSUIVIS

2.1. NECESSITE DE LEGIFERER

La nécessité de légiférer provient ici de l'obligation constitutionnelle de transposition en droit interne d'une directive imposée par l'article 88-1 de la Constitution qui dispose que « [l]a République participe à l'Union européenne ». Cette obligation a d'ailleurs été rappelée par le Conseil constitutionnel dans le considérant 7 de sa décision n° 2004-496 DC du 10 juin 2004 : « Considérant qu'aux termes de l'article 88-1 de la Constitution […] ; qu'ainsi, la transposition en droit interne d'une directive communautaire résulte d'une exigence constitutionnelle à laquelle il ne pourrait être fait obstacle qu'en raison d'une disposition expresse contraire de la Constitution ».

2.2. OBJECTIFS POURSUIVIS

Le présent article permet de transposer, à l'article L. 533-10-4 du code monétaire et financier relatif aux obligations des prestataires de services d'investissement, les exigences rendues applicables par le chapitre II du règlement DORA en matière d'objectifs assignés aux 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.

De plus, il permet d'introduire une obligation de mise en œuvre de politiques et de plans en matière de continuité des activités liées aux technologies de l'information et de la communication, et de plans de réponse et de rétablissement des technologies de l'information et de la communication conformément au règlement DORA.

3. OPTIONS POSSIBLES ET DISPOSITIF RETENU

3.1. OPTIONS ENVISAGEES

Aucune autre option n'a été envisagée dans la mesure où cette disposition est commandée par une norme supérieure issue du droit de l'Union européenne.

3.2. OPTION RETENUE

La directive DORA ne prévoit que des modifications d'ordre technique des différentes directives sectorielles qui visent à assurer la cohérence avec les nouvelles exigences introduites par le règlement DORA. Il a ainsi été décidé de transposer textuellement l'article 6,2), a) de la directive DORA à l'article L. 533-10-4 du code monétaire et financier.

Il est en effet proposé de modifier l'article L. 533-10-4 du code monétaire et financier relatif aux obligations des prestataires de services d'investissement en rajoutant dans le 1° a) la mention des exigences fixées au chapitre II du règlement DORA (ce qui correspond à une transposition de l'article 6,2), a) de la directive DORA sur le trading algorithmique) et en transposant dans le 2° la rédaction présente dans l'article 6,2), a) de la directive DORA sur des « mécanismes de continuité des activités efficaces (…) y compris d'une politique et de plans en matière de continuité des activités liées aux technologies de l'information et de la communication et de plans de réponse et de rétablissement des TIC mis en place conformément à l'article 11 du règlement (UE) 2022/2554 … » lesquels doivent être conformes aux exigences prévues par le chapitres II et IV du règlement DORA.

4. ANALYSE DES IMPACTS DES DISPOSITIONS ENVISAGEES

4.1. IMPACTS JURIDIQUES

4.1.1. Impacts sur l'ordre juridique interne

Le présent article modifie l'article L. 533-10-4 du code monétaire et financier.

4.1.2. Articulation avec le droit international et le droit de l'Union européenne

Cet article est conforme au droit européen, consistant en une reprise *in extenso* de l'article 6.2 de la directive DORA.

4.2. IMPACTS ECONOMIQUES ET FINANCIERS

4.2.1. Impacts macroéconomiques

Néant.

4.2.2. Impacts sur les entreprises

Les entreprises d'investissement recourant au trading algorithmique doivent mettre à jour leurs systèmes de contrôles des risques pour garantir la résilience et une capacité suffisante de leurs systèmes de négociation conformément aux exigences fixées au chapitre II du règlement

DORA. De même, elles doivent enrichir leurs mécanismes de continuité des activités en mettant en place une politique et des plans en matière de continuité des activités liées aux TIC. De même, elles doivent disposer de plans de réponse et de rétablissement des TIC.

4.2.3. Impacts budgétaires

Néant.

4.3. IMPACTS SUR LES COLLECTIVITES TERRITORIALES

Néant. S'agissant d'articles relatifs au droit monétaire, bancaire et financier, le présent article est sans incidence sur le fonctionnement des collectivités territoriales.

4.4. IMPACTS SUR LES SERVICES ADMINISTRATIFS

Néant.

4.5. IMPACTS SOCIAUX

4.5.1. Impacts sur la société

Néant.

4.5.2. Impacts sur les personnes en situation de handicap

Néant.

4.5.3. Impacts sur l'égalité entre les femmes et les hommes

Néant.

4.5.4. Impacts sur la jeunesse

Néant.

4.5.5. Impacts sur les professions réglementées

Néant.

4.6. IMPACTS SUR LES PARTICULIERS

Néant.

4.7. IMPACTS ENVIRONNEMENTAUX

Néant.

5. CONSULTATIONS ET MODALITES D'APPLICATION

5.1. CONSULTATIONS MENEES

En application de l'article L. 614-2 du code monétaire et financier, le Comité consultatif de la législation et de la réglementation financières (CCLRF) a été consulté a rendu un avis favorable le 23 mai 2024.

La rédaction proposée a en outre été envoyée pour information et sur base informelle à l'Autorité des marchés financiers.

5.2. MODALITES D'APPLICATION

5.2.1. Application dans le temps

Le présent article s'appliquera à compter du 17 janvier 2025 conformément à l'article 62 du présent projet de loi.

5.2.2. Application dans l'espace

La mesure s'applique à l'ensemble du territoire de la République.

Elle s'applique de plein droit aux collectivités territoriales régies par l'article 73 de la Constitution (Guadeloupe, Guyane, Martinique, La Réunion et Mayotte) et certaines des collectivités relevant de l'article 74 (Saint-Barthélemy, Saint Martin et Saint-Pierre-et-Miquelon).

L'article 4 de la loi du 29 juillet 1961, l'article 7 de la loi organique n° 2004-192 du 27 février 2004 portant statut d'autonomie de la Polynésie Française et l'article 6-2 de la loi n° 99-209 organique du 19 mars 1999 relative à la Nouvelle-Calédonie soumettent respectivement pour les Îles Wallis et Futuna, la Polynésie Française et la Nouvelle-Calédonie au principe de spécialité législative, les lois et règlements n'y étant applicables que sur mention expresse, dès

lors qu'ils interviennent dans un domaine pour lequel l'Etat est compétent. En effet, l'Etat est compétent en matière bancaire et financière dans ces collectivités ultramarines régies par le principe de spécialité législative où toute création ou modification du code précité doit être rendue applicable par mention expresse.

Ainsi, l'article 56 du projet de loi rend applicables les présentes dispositions en Nouvelle-Calédonie, en Polynésie française et dans les îles Wallis et Futuna en modifiant les articles L. 773-30, L. 774-30 et L. 775-24 du code monétaire et financier.

Enfin, la modification de l'article L. 712-7 du code monétaire et financier réalisée par l'article 56 du projet de loi rend applicable le règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier à Saint-Pierre et Miquelon, en Nouvelle-Calédonie, en Polynésie française et dans les îles Wallis et Futuna qui sont des pays et territoires d'outre-mer où le droit de l'Union européenne ne s'applique pas.

Par coordination, l'article L. 771-1 est complété par les références au règlement (UE) 2022/2554 précité.

5.2.3. Textes d'application

Le présent article ne requiert aucune mesure d'application.

Article 53 – Référence aux prestataires informatiques critiques au sein des tiers auxquels l'Autorité de contrôle prudentiel et de résolution peut demander toute information

1. ÉTAT DES LIEUX

1.1. CADRE GENERAL

L'article 65(3) de la 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, ci-après « directive CRD », prévoit notamment que les autorités de supervision sont investies de tous les pouvoirs de collecte d'informations nécessaires à l'exercice de leurs fonctions à l'égard d'une liste de personnes physiques et morales soumises à leur contrôle (établissements de crédit tels que définis au I de l'article L. 511-1 du code monétaire et financier, compagnies financières holding, compagnies financières holding mixtes notamment).

L'article 4(1) de la 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, ci-après « directive DORA », modifie cet article 65(3) de la directive CRD afin d'ajouter à la liste des personnes susceptibles de fournir toute information nécessaire aux autorités de supervision les prestataires tiers de services fondés sur les technologies de l'information et de la communication (TIC) visés au chapitre V du règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) n° 1060/2009, (UE) n° 648/2012, (UE) n° 600/2014, (UE) n° 909/2014 et (UE) 2016/1011, ci-après « règlement DORA », auprès desquels les entités soumises à supervision ont externalisé des fonctions ou des activités.

L'article L. 612-24 du code monétaire et financier relatif aux informations que l'Autorité de contrôle prudentiel et de résolution (ACPR)[271] est habilitée à demander dans le cadre de l'exercice de ses pouvoirs de contrôle prévoit déjà aujourd'hui que le secrétaire général de l'ACPR peut demander toute information nécessaire à l'accomplissement de ses missions (par

[271] Conformément à l'article L. 612-1 du code monétaire et financier, l'ACPR « veille à la préservation de la stabilité du système financier et à la protection des clients, assurés, adhérents et bénéficiaires » des banques et des compagnies d'assurance. Elle contrôle également « le respect par ces personnes des dispositions européennes qui leur sont directement applicables » ainsi que leur respect des dispositions législatives et réglementaires de droit national.

exemple, des rapports d'audit interne ou une copie d'un contrat contractuel signé par l'entité assujettie) aux tiers auprès desquels les entités assujetties à son contrôle[272] ont externalisé des fonctions ou activités opérationnelles. Ces fonctions ou activités concernent à la fois des activités initialement exécutées par l'entité assujettie puis confiées à un prestataire externe ainsi que le soutien d'activités nouvellement opérées par l'entité et directement sous-traitées par un prestataire. Ce recours à l'externalisation peut notamment porter sur la gestion des réseaux et systèmes d'information ou l'hébergement de données de l'entité assujettie.

Le présent article du projet de loi modifie l'article L. 612-24 du code monétaire et financier afin de préciser que les prestataires tiers critiques de services fondés sur les technologies de l'information et de la communication (tels que désignés en application du règlement DORA) comptent parmi les personnes auxquelles le secrétaire général de l'ACPR peut demander tous renseignements et documents. Ces dispositions sont aussi applicables aux prestataires auprès desquels les sociétés de financement (telles que définies au II de l'article L. 511-1 du code monétaire et financier) ont externalisé des fonctions ou activités.

1.2. CADRE CONSTITUTIONNEL

Aux termes de l'article 88-1 de la Constitution : « La République participe aux Communautés européennes et à l'Union européenne, constituées d'Etats qui ont choisi librement, en vertu des traités qui les ont instituées, d'exercer en commun certaines de leurs compétences ». Le Conseil constitutionnel déduit de cette disposition que : « la transposition en droit interne d'une directive communautaire résulte d'une exigence constitutionnelle »[273]. Il en va de même pour une loi ayant pour objet d'adapter le droit interne à un règlement de l'Union européenne[274].

En tout état de cause, la mesure relève du domaine de la loi en application de l'article 34 de la Constitution, au titre des obligations civiles et commerciales.

1.3. CADRE CONVENTIONNEL

[272] Conformément à l'article L. 612-2 du code monétaire et financier, les entités relevant de la compétence de l'ACPR appartiennent à la fois au secteur de la banque, des services de paiement et des services d'investissement (à l'instar des établissements de crédit, des sociétés de financement, des chambres de compensation ou des changeurs manuels) ainsi qu'au secteur de l'assurance (incluant les activités de réassurance, les instituts de prévoyance, les fonds de retraite professionnelle ou les mutuelles). En ce qui con concerne le secteur bancaire, au 31 décembre 2021, 769 entités relevaient du périmètre de supervision de l'ACPR (source : rapport annuel de l'ACPR au titre de l'exercice 2021).

[273] Voir notamment la décision n° 2004-496 DC du 10 juin 2004, « Loi pour la confiance dans l'économie numérique ».

[274] Voir par exemple la décision n° 2018-765, « Loi relative à la protection des données personnelles », considérant 3.

Le règlement européen DORA précité, adopté à l'automne 2022 et entré en vigueur le 16 janvier 2023, renforce les obligations opérationnelles s'imposant aux principaux acteurs du secteur financier. Il est complété par la directive éponyme, également susmentionnée, qui regroupe une série de dispositions techniques, visant à clarifier les obligations et à actualiser les références aux enjeux de résilience opérationnelle au sein des directives qui préexistaient au règlement DORA. L'article 4 de la directive DORA liste les amendements apportés à la directive CRD relative encadrant les activités des établissements de crédit et harmonisant leur surveillance prudentielle.

1.4. ÉLEMENTS DE DROIT COMPARE

Les autres Etats-membres de l'Union européenne modifieront également leur droit national conformément à la directive DORA afin d'introduire une référence aux prestataires informatiques critiques au sein des tiers auxquels leurs autorités de supervision nationales compétentes peuvent demander des informations.

2. NECESSITE DE LEGIFERER ET OBJECTIFS POURSUIVIS

2.1. NECESSITE DE LEGIFERER

La nécessité de légiférer provient ici tout d'abord de l'obligation constitutionnelle de transposition en droit interne d'une directive imposée par l'article 88-1 de la Constitution qui dispose que « [l]a République participe à l'Union européenne ». Cette obligation a d'ailleurs été rappelée par le Conseil constitutionnel dans le considérant 7 de sa décision n°2004-496 DC du 10 juin 2004 : « Considérant qu'aux termes de l'article 88-1 de la Constitution […] ; qu'ainsi, la transposition en droit interne d'une directive communautaire résulte d'une exigence constitutionnelle à laquelle il ne pourrait être fait obstacle qu'en raison d'une disposition expresse contraire de la Constitution ».

2.2. OBJECTIFS POURSUIVIS

Cet article vise à transposer dans le code monétaire et financier les dispositions des articles 4(1) de la directive DORA, en précisant que les prestataires tiers critiques de services fondés sur les technologies de l'information et de la communication visés par le règlement DORA comptent parmi les personnes auxquelles le secrétaire général de l'Autorité de contrôle prudentiel et de résolution (ACPR) peut demander tous renseignements et documents. Il rend également ces dispositions applicables aux prestataires tiers critiques au sens de DORA auprès desquels les sociétés de financement ont externalisé des fonctions ou activités.

3. OPTIONS POSSIBLES ET DISPOSITIF RETENU

3.1. OPTIONS ENVISAGEES

Suivant le principe du parallélisme des formes, une disposition législative ne peut être modifiée que par une mesure de même niveau normatif. Ainsi, aucune autre option que le recours à la loi n'a été envisagée ici.

3.2. OPTION RETENUE

La directive DORA ne prévoit que des modifications d'ordre technique des différentes directives sectorielles qui visent à assurer la cohérence avec les nouvelles exigences introduites par le règlement DORA. Dans un souci de simplicité et dans la mesure où la transposition de cette directive DORA est sans enjeu majeur, il a été décidé d'introduire les modifications afférentes dans les dispositions de droit interne transposant la directive sectorielle CRD applicable aux établissements de crédit. L'article L. 612-24 du code monétaire et financier est ainsi modifié. Ces dispositions de droit interne étant aussi applicables aux sociétés de financement, aucune modification supplémentaire n'a été nécessaire pour leur appliquer ces nouvelles dispositions européennes.

4. ANALYSE DES IMPACTS DES DISPOSITIONS ENVISAGEES

4.1. IMPACTS JURIDIQUES

4.1.1. Impacts sur l'ordre juridique interne

L'article L. 612-24 du code monétaire et financier est modifié.

4.1.2. Articulation avec le droit international et le droit de l'Union européenne

Cet article vise à transposer des dispositions du droit de l'Union européenne dans le droit interne.

L'article 65(3) de la directive CRD prévoit que les autorités de supervision sont investies de tous les pouvoirs de collecte d'informations nécessaires à l'exercice de leurs fonctions à l'égard d'une liste de personnes physiques et morales soumises à leur contrôle. L'article 4(1) de la directive DORA, modifie cet article 65(3) de la directive CRD afin d'ajouter à la liste des personnes susceptibles de fournir toute information nécessaire aux autorités de supervision les prestataires tiers de services fondés sur les TIC visés au chapitre V du règlement DORA, auprès desquels les entités soumises à supervision ont externalisé des

fonctions ou des activités. L'article L. 612-24 du code monétaire et financier relatif aux informations que l'ACPR est habilitée à demander dans le cadre de l'exercice de ses pouvoirs de contrôle prévoit déjà aujourd'hui que le secrétaire général de l'ACPR peut demander toute information nécessaire à l'accomplissement de ses missions aux tiers auprès desquels les entités assujetties à son contrôle ont externalisé des fonctions ou activités opérationnelles.

Le présent article du projet de loi modifie l'article L. 612-24 du code monétaire et financier afin de préciser que les prestataires tiers critiques de services fondés sur les TIC comptent parmi les personnes auxquelles le secrétaire général de l'ACPR peut demander tous renseignements et documents. Ces dispositions sont aussi applicables aux prestataires auprès desquels les sociétés de financement ont externalisé des fonctions ou activités.

4.2. IMPACTS ECONOMIQUES ET FINANCIERS

4.2.1. Impacts macroéconomiques

Sans objet.

4.2.2. Impacts sur les entreprises

Il sera désormais précisé que les prestataires tiers critiques de services fondés sur les technologies de l'information et de la communication des établissements de crédit et des sociétés de financement visés par le règlement DORA comptent parmi les personnes auxquelles le secrétaire général de l'Autorité de contrôle prudentiel et de résolution (ACPR) peut demander tous renseignements et documents. L'identité et le nombre de ces prestataires tiers critiques établis à l'appréciation des autorités européennes de surveillance en application de l'article 31 du règlement DORA.

Toutefois l'article L. 612-24 du code monétaire et financier prévoit déjà le pouvoir du secrétaire de l'ACPR de demander aux tiers auprès desquels les entités assujetties à son contrôle ont externalisé des fonctions ou activités opérationnelles toute information nécessaires à l'accomplissement de son contrôle. Aussi, cette modification apportée à l'article L. 612-24 du code monétaire et financier ne devrait pas avoir d'impact majeur par rapport à la situation existante.

4.2.3. Impacts budgétaires

Sans objet.

4.3. IMPACTS SUR LES COLLECTIVITES TERRITORIALES

Sans objet.

4.4. IMPACTS SUR LES SERVICES ADMINISTRATIFS

Le secrétaire de l'ACPR disposant déjà aujourd'hui du pouvoir de demander aux tiers auprès desquels les entités assujetties à son contrôle ont externalisé des fonctions ou activités opérationnelles toute information nécessaires à l'accomplissement de son contrôle. En conséquence, cette modification apportée à l'article L. 612-24 du code monétaire et financier ne devrait pas avoir d'impact majeur sur l'exercice du contrôle de l'ACPR. Par ailleurs, la précision apportée par le présent article ne vise que les prestataires qui auront été désignés critiques par les autorités européennes de surveillance en application du règlement DORA ; leur nombre sera par définition restreint à un segment particulièrement sensible pour la stabilité financière au sein de la population des prestataires fournissant des services informatiques au secteur financier.

4.5. IMPACTS SOCIAUX

4.5.1. Impacts sur la société

Sans objet.

4.5.2. Impacts sur les personnes en situation de handicap

Sans objet.

4.5.3. Impacts sur l'égalité entre les femmes et les hommes

Sans objet.

4.5.4. Impacts sur la jeunesse

Sans objet.

4.5.5. Impacts sur les professions réglementées

Sans objet.

4.6. IMPACTS SUR LES PARTICULIERS

Sans objet.

4.7. IMPACTS ENVIRONNEMENTAUX

Sans objet.

5. CONSULTATIONS ET MODALITES D'APPLICATION

5.1. CONSULTATIONS MENEES

En application de l'article L. 614-2 du code monétaire et financier, le Comité consultatif de la législation et de la réglementation financières (CCLRF) a été consulté a rendu un avis favorable le 23 mai 2024.

Elle a en outre été soumise à l'avis des services de l'Autorité de contrôle prudentiel et de résolution (ACPR) et de l'Association française des Sociétés Financières (ASF).

5.2. MODALITES D'APPLICATION

5.2.1. Application dans le temps

Le présent article s'appliquera à compter du 17 janvier 2025 conformément à l'article 62 du présent projet de loi.

5.2.2. Application dans l'espace

La mesure s'applique à l'ensemble du territoire de la République.

Elle s'applique de plein droit aux collectivités territoriales régies par l'article 73 de la Constitution (Guadeloupe, Guyane, Martinique, La Réunion et Mayotte) et certaines des collectivités relevant de l'article 74 (Saint-Barthélemy, Saint Martin et Saint-Pierre-et-Miquelon).

L'article 4 de la loi du 29 juillet 1961, l'article 7 de la loi organique n° 2004-192 du 27 février 2004 portant statut d'autonomie de la Polynésie Française et l'article 6-2 de la loi n° 99-209 organique du 19 mars 1999 relative à la Nouvelle-Calédonie soumettent respectivement pour les Îles Wallis et Futuna, la Polynésie Française et la Nouvelle-Calédonie au principe de spécialité législative, les lois et règlements n'y étant applicables que sur mention expresse, dès lors qu'ils interviennent dans un domaine pour lequel l'Etat est compétent. En effet, l'Etat est compétent en matière bancaire et financière dans ces collectivités ultramarines régies par le principe de spécialité législative où toute création ou modification du code précité doit être rendue applicable par mention expresse.

Ainsi, l'article 56 du projet de loi rend applicables les présentes dispositions en Nouvelle-Calédonie, en Polynésie française et dans les îles Wallis et Futuna en modifiant les articles L. 783-2, L. 784-2 et L. 785-2 du code monétaire et financier.

Enfin, la modification de l'article L. 712-7 du code monétaire et financier réalisée par l'article 56 du projet de loi rend applicable le règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier à Saint-Pierre et Miquelon, en Nouvelle-Calédonie, en Polynésie française et dans les îles Wallis et Futuna qui sont des pays et territoires d'outre-mer où le droit de l'Union européenne ne s'applique pas.

Par coordination, l'article L. 781-1 est complété par les références au règlement (UE) 2022/2554 précité.

5.2.3. Textes d'application

Le présent article ne requiert aucune mesure d'application.

Article 54 – Référence à la résilience opérationnelle numérique au sein des plans préventifs de résolution des établissements de crédit et des sociétés de financement

1. ÉTAT DES LIEUX

1.1. CADRE GENERAL

La résilience opérationnelle numérique[275] est essentielle pour préserver les fonctions critiques et les activités fondamentales[276] d'une entité financière en cas de résolution et éviter ainsi de perturber l'économie réelle et le système financier. Afin qu'elle corresponde aux objectifs du cadre de l'Union en matière de résilience opérationnelle, l'article 5 de la 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, ci-après « directive DORA », modifie la directive 2014/59/UE dite « BRRD »[277], notamment son article 10, en vue de garantir que les informations relatives à la résilience opérationnelle sont prises en compte dans le contexte de la planification de la résolution et de l'évaluation de la résolvabilité des entités financières. Cette planification est assurée par le Conseil de résolution unique et par les autorités de résolution nationale auprès des entités assujetties à la directive BRRD. En droit français, l'ACPR remplit les fonctions d'autorité de résolution nationale en application du 4° de l'article L. 612-1 du code monétaire

[275] Définie à l'article 3(1) du règlement DORA de la façon suivante : « la capacité d'une entité financière à développer, garantir et réévaluer son intégrité et sa fiabilité opérationnelles en assurant directement ou indirectement par le recours aux services fournis par des prestataires tiers de services TIC, l'intégralité des capacités liées aux TIC nécessaires pour garantir la sécurité des réseaux et des systèmes d'information qu'elle utilise, et qui sous-tendent la fourniture continue de services financiers et leur qualité, y compris en cas de perturbation ».

[276] Les fonctions critiques et les activités fondamentales d'une entité financière sont respectivement définies aux article 2(35) et 2(36) de la directive dite BRRD. Les fonctions critiques sont les activités, services ou opérations dont l'interruption est susceptible, dans un ou plusieurs États membres, d'entraîner des perturbations des services indispensables à l'économie réelle ou de perturber la stabilité financière en raison de la taille ou de la part de marché de l'établissement ou du groupe, de son interdépendance interne et externe, de sa complexité ou des activités transfrontières qu'il exerce, une attention particulière étant accordée à la substituabilité de ces activités, services ou opérations. Les activités fondamentales sont les activités et services associés qui représentent pour un établissement ou pour un groupe dont un établissement fait partie des sources importantes de revenus, de bénéfices ou de valeur de franchise.

[277] 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.

et financier. A ce titre, elle veille à l'élaboration et la mise en œuvre des mesures de prévention et de résolution des crises bancaires et des crises dans le secteur de l'assurance.

Le présent article permet de transposer les points a) et b) de l'article 5(1) de la directive DORA et modifie ainsi les dispositions de l'article L. 613-38 du code monétaire et financier relatives aux plans préventifs de résolution que doivent développer les autorités de résolution des établissements de crédit et les entreprises d'investissement (tels que définis respectivement par les articles L. 511-1 et L. 531-4 et suivants du code monétaire et financier). Conformément à l'article 10 de la directive BRRD, les plans préventifs de résolution définissent les mesures que l'autorité de résolution peut prendre si l'entité financière est défaillante ou susceptible de l'être. Dans le détail, le présent article introduit d'abord la nécessité de montrer au sein de ces plans comment les modalités de dissociation économiques et juridiques des fonctions critiques par rapport aux autres fonctions (c'est-à-dire l'exercice des différents pouvoirs de résolution à l'instar de la cession des activités, la constitution d'un établissement-relais ou une mesure de séparation des actifs) assurent, en plus de la continuité de ces fonctions, la résilience opérationnelle numérique en cas de défaillance de l'entité. Il précise également que la description, au sein de ces plans, des principaux systèmes et opérations permettant de maintenir le fonctionnement permanent des processus opérationnels de l'entité financière doit aussi inclure la description de ceux permettant de maintenir le fonctionnement des réseaux et systèmes d'information visés par le 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, ci-après « règlement DORA ».

1.2. CADRE CONSTITUTIONNEL

Aux termes de l'article 88-1 de la Constitution : « La République participe aux Communautés européennes et à l'Union européenne, constituées d'Etats qui ont choisi librement, en vertu des traités qui les ont instituées, d'exercer en commun certaines de leurs compétences ». Le Conseil constitutionnel déduit de cette disposition que : « la transposition en droit interne d'une directive communautaire résulte d'une exigence constitutionnelle »[278]. Il en va de même pour une loi ayant pour objet d'adapter le droit interne à un règlement de l'Union européenne[279].

[278] Voir notamment la décision n° 2004-496 DC du 10 juin 2004, « Loi pour la confiance dans l'économie numérique ».

[279] Voir par exemple la décision n° 2018-765, « Loi relative à la protection des données personnelles », considérant 3.

En tout état de cause, la mesure relève du domaine de la loi en application de l'article 34 de la Constitution, au titre des obligations civiles et commerciales.

1.3. CADRE CONVENTIONNEL

Le règlement européen DORA, adopté à l'automne 2022 et entré en vigueur le 16 janvier 2023, renforce les obligations opérationnelles s'imposant aux principaux acteurs du secteur financier. Il est complété par la directive éponyme qui regroupe une série de dispositions techniques, visant à clarifier les obligations et à actualiser les références aux enjeux de résilience opérationnelle au sein des directives qui préexistaient au règlement DORA. L'article 5 de la directive DORA liste les amendements apportés à la directive BRRD établissant un cadre pour le redressement et la résolution des établissements de crédit et des entreprises d'investissement. En particulier, l'article 10 détaille la finalité et le contenu des plans de résolution que les autorités de résolution doivent développer pour chacune des entités financières assujetties.

1.4. ÉLEMENTS DE DROIT COMPARE

Les autres Etats-membres de l'Union européenne modifieront également leur droit national conformément à la directive DORA afin d'introduire une référence à la résilience opérationnelle numérique au sein des plans préventifs de résolution des établissements de crédit.

2. NECESSITE DE LEGIFERER ET OBJECTIFS POURSUIVIS

2.1. NECESSITE DE LEGIFERER

La nécessité de légiférer provient ici tout d'abord de l'obligation constitutionnelle de transposition en droit interne d'une directive imposée par l'article 88-1 de la Constitution qui dispose que « [l]a République participe à l'Union européenne ». Cette obligation a d'ailleurs été rappelée par le Conseil constitutionnel dans le considérant 7 de sa décision n° 2004-496 DC du 10 juin 2004 : « Considérant qu'aux termes de l'article 88-1 de la Constitution […] ; qu'ainsi, la transposition en droit interne d'une directive communautaire résulte d'une exigence constitutionnelle à laquelle il ne pourrait être fait obstacle qu'en raison d'une disposition expresse contraire de la Constitution ».

2.2. OBJECTIFS POURSUIVIS

Cet article vise à transposer les points a) et b) de l'article 5(1) de la directive DORA en introduisant d'abord à l'article L. 613-38 du code monétaire et financier la nécessité de montrer au sein des plans préventifs de résolution comment les modalités de dissociation économiques et juridiques des fonctions critiques par rapport aux autres fonctions assurent, en plus de la continuité de ces fonctions, la résilience opérationnelle numérique en cas de défaillance de l'entité. Il précise également que la description, au sein de ces plans, des principaux systèmes et opérations permettant de maintenir le fonctionnement permanent des processus opérationnels de l'entité financière doit aussi inclure la description de ceux permettant de maintenir le fonctionnement des réseaux et systèmes d'information visés par le règlement DORA.

3. OPTIONS POSSIBLES ET DISPOSITIF RETENU

3.1. OPTIONS ENVISAGEES

Suivant le principe du parallélisme des formes, une disposition législative ne peut être modifiée que par une mesure de même niveau normatif. Ainsi, aucune autre option que le recours à la loi n'a été envisagée ici.

3.2. OPTION RETENUE

La directive DORA ne prévoit que des modifications d'ordre technique des différentes directives sectorielles qui visent à assurer la cohérence avec les nouvelles exigences introduites par le règlement DORA. Dans un souci de simplicité et dans la mesure où la transposition de cette directive DORA est sans enjeu majeur, il a été décidé d'introduire les modifications afférentes dans les dispositions de droit interne pertinentes transposant celles de la directive sectorielle BRRD. Ainsi, l'article L. 613-38 du code monétaire et financier est modifié.

4. ANALYSE DES IMPACTS DES DISPOSITIONS ENVISAGEES

4.1. IMPACTS JURIDIQUES

4.1.1. Impacts sur l'ordre juridique interne

L'article L. 613-38 du code monétaire et financier est modifié.

4.1.2. Articulation avec le droit international et le droit de l'Union européenne

Cet article vise à transposer des dispositions du droit de l'Union européenne dans le droit interne.

L'article 5 de la directive DORA modifie la directive BRRD, notamment son article 10, en vue de garantir que les informations relatives à la résilience opérationnelle soient prises en compte dans le contexte de la planification de la résolution et de l'évaluation de la résolvabilité des entités financières.

Le présent article permet de transposer les points a) et b) de l'article 5(1) de la directive DORA et modifie ainsi les dispositions de l'article L. 613-38 du code monétaire et financier relatives aux plans préventifs de résolution que doivent développer les autorités de résolution des établissements de crédit et les entreprises d'investissement. Dans le détail, il introduit d'abord la nécessité de montrer au sein de ces plans comment les modalités de dissociation économiques et juridiques des fonctions critiques par rapport aux autres fonctions assurent, en plus de la continuité de ces fonctions, la résilience opérationnelle numérique en cas de défaillance de l'entité. Il précise également que la description, au sein de ces plans, des principaux systèmes et opérations permettant de maintenir le fonctionnement permanent des processus opérationnels de l'entité financière doit aussi inclure la description de ceux permettant de maintenir le fonctionnement des réseaux et systèmes d'information visés par le règlement DORA.

4.2. IMPACTS ECONOMIQUES ET FINANCIERS

4.2.1. Impacts macroéconomiques

Sans objet.

4.2.2. Impacts sur les entreprises

Sans objet.

4.2.3. Impacts budgétaires

Sans objet.

4.3. IMPACTS SUR LES COLLECTIVITES TERRITORIALES

Sans objet.

4.4. IMPACTS SUR LES SERVICES ADMINISTRATIFS

L’entrée en vigueur de ces nouvelles obligations en matière de cyber-résilience dans le secteur financier va avoir des répercussions sur l’activité de l’Autorité de contrôle prudentiel et de résolution (ACPR) et sur ses besoins en termes de ressources budgétaires et d’effectifs.

Cet article se traduira par une plus grande prise en compte par les services de l’ACPR de la résilience opérationnelle numérique et des réseaux et systèmes d’information visés par le règlement DORA au moment d’établir les plans préventifs de résolution.

4.5. IMPACTS SOCIAUX

4.5.1. Impacts sur la société

Sans objet.

4.5.2. Impacts sur les personnes en situation de handicap

Sans objet.

4.5.3. Impacts sur l’égalité entre les femmes et les hommes

Sans objet.

4.5.4. Impacts sur la jeunesse

Sans objet.

4.5.5. Impacts sur les professions réglementées

Sans objet.

4.6. IMPACTS SUR LES PARTICULIERS

Sans objet.

4.7. IMPACTS ENVIRONNEMENTAUX

Sans objet.

5. CONSULTATIONS ET MODALITES D’APPLICATION

5.1. CONSULTATIONS MENEES

En application de l'article L. 614-2 du code monétaire et financier, le Comité consultatif de la législation et de la réglementation financières (CCLRF) a été consulté a rendu un avis favorable le 23 mai 2024.

La rédaction proposée a en outre été soumise pour information et sur base informelle aux services de l'Autorité de contrôle prudentiel et de résolution (ACPR) et à l'Association française des Sociétés Financières (ASF).

5.2. MODALITES D'APPLICATION

5.2.1. Application dans le temps

Les dispositions du titre III s'appliqueront à compter du 17 janvier 2025 conformément à l'article 62 du présent projet de loi.

Toutefois, afin d'accorder un délai de mise en œuvre supplémentaire pour les sociétés de financement considérées comme de taille petite et non-complexes et dont les moyens et ressources sont réputées moins importantes, l'article 62 du projet de loi introduit une entrée en application différée – repoussée d'un an au 17 janvier 2026 – du présent article pour les sociétés de financement remplissant les conditions prévues au point 145 du paragraphe 1 de l'article 4 du règlement (UE) n° 575/2013 du Parlement européen et du Conseil dit « CRR » qui définit les établissements de petite taille et non complexe.

Pour rappel, un établissement de petite taille et non complexe est un établissement qui remplit toutes les conditions suivantes :

a) il ne s'agit pas d'un établissement de grande taille ;

b) la valeur totale de ses actifs sur base individuelle ou, le cas échéant, sur base consolidée conformément au présent règlement et à la directive 2013/36/UE est en moyenne égale ou inférieure à un seuil de cinq milliards d'euros sur la période de quatre ans qui précède immédiatement la période de déclaration annuelle en cours; les États membres peuvent abaisser ce seuil ;

c) 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 conformément à l'article 4 de la directive 2014/59/UE ;

d) son portefeuille de négociation est classé comme étant de faible taille au sens de l'article 94, paragraphe 1 du règlement CRR ;

e) la valeur totale de ses positions sur 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 %, ces deux pourcentages étant calculés conformément à l'article 273 bis, paragraphe 3 ;

f) plus de 75 % du total des actifs et des passifs consolidés de l'établissement, à l'exclusion, dans les deux cas, des expositions intragroupe, sont liés à des activités avec des contreparties situées dans l'Espace économique européen ;

g) l'établissement n'utilise pas de modèles internes pour satisfaire aux exigences prudentielles prévues par le présent règlement, 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 prévues à l'article 433 bis ou 433 quater du règlement CRR sur base consolidée ;

h) 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 ;

i) 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.

Les sociétés de financement remplissant ces conditions sont a priori au nombre de 135. Cette définition d'établissement de petite taille et non complexe s'applique bien aux sociétés de financement puisque les dispositions du règlement européen CRR concerne également cette catégorie d'entité en application de l'article 2 de l'arrêté du 23 novembre 2023 relatif au régime prudentiel des sociétés de financement.

Ainsi, les sociétés de financement ne remplissant pas ces conditions et considérées comme les plus importantes en termes de taille (dont la valeur totale des actifs serait supérieure cinq milliards d'euros, soit une dizaine de sociétés visées) devront appliquer les exigences découlant de la directive et du règlement DORA dès l'entrée en vigueur des dispositions pertinentes de ce projet de loi.

5.2.2. Application dans l'espace

La mesure s'applique à l'ensemble du territoire de la République.

Elle s'applique de plein droit aux collectivités territoriales régies par l'article 73 de la Constitution (Guadeloupe, Guyane, Martinique, La Réunion et Mayotte) et certaines des collectivités relevant de l'article 74 (Saint-Barthélemy, Saint Martin et Saint-Pierre-et-Miquelon).

L'article 4 de la loi du 29 juillet 1961, l'article 7 de la loi organique n° 2004-192 du 27 février 2004 portant statut d'autonomie de la Polynésie Française et l'article 6-2 de la loi n° 99-209

organique du 19 mars 1999 relative à la Nouvelle-Calédonie soumettent respectivement pour les Îles Wallis et Futuna, la Polynésie Française et la Nouvelle-Calédonie au principe de spécialité législative, les lois et règlements n'y étant applicables que sur mention expresse, dès lors qu'ils interviennent dans un domaine pour lequel l'Etat est compétent. En effet, l'Etat est compétent en matière bancaire et financière dans ces collectivités ultramarines régies par le principe de spécialité législative où toute création ou modification du code précité doit être rendue applicable par mention expresse.

Ainsi, l'article 56 du projet de loi rend applicables les présentes dispositions en Nouvelle-Calédonie, en Polynésie française et dans les îles Wallis et Futuna en modifiant les articles L. 783-4, L. 784-4 et L. 785-4 du code monétaire et financier.

Enfin, la modification de l'article L. 712-7 du code monétaire et financier réalisée par l'article 56 du projet de loi rend applicable le règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier à Saint-Pierre et Miquelon, en Nouvelle-Calédonie, en Polynésie française et dans les îles Wallis et Futuna qui sont des pays et territoires d'outre-mer où le droit de l'Union européenne ne s'applique pas.

Par coordination, l'article L. 781-1 est complété par les références au règlement (UE) 2022/2554 précité.

5.2.3. Textes d'application

Le présent article ne requiert aucune mesure d'application.

Article 55 – Extension de la liste des autorités habilitées à s'échanger des informations

1. ÉTAT DES LIEUX

1.1. CADRE GENERAL

L'article L. 631-1 du code monétaire et financier régit la coopération et les échanges d'informations entre autorités dans le domaine financier, ce qui recouvre la Banque de France, l'Institut d'émission des départements d'outre-mer (IEDOM), l'Institut d'émission d'outre-mer (IEOM), l'Autorité de contrôle prudentiel et de résolution (ACPR) et l'Autorité des marchés financiers (AMF).

A ce titre, le quatrième alinéa du II de l'article L. 631-1 du code monétaire et financier prévoit que l'Autorité des marchés financiers et l'ANSSI sont habilitées à se communiquer les renseignements utiles à l'exercice de leurs missions respectives dans le domaine de la sécurité des systèmes d'information.

Par ailleurs, le II de l'article L. 521-10 du code monétaire et financier prévoit que la Banque de France, si elle l'estime nécessaire, informe l'ACPR de tout incident de sécurité majeur, en application de l'article L. 631-1 du même code.

Il est proposé de modifier, en conséquence, le quatrième alinéa du II de l'article L. 631-1 du code monétaire et financier afin d'y inclure la Banque de France et l'Autorité de contrôle prudentiel et de résolution.

1.2. CADRE CONSTITUTIONNEL

Aux termes de l'article 88-1 de la Constitution : « La République participe aux Communautés européennes et à l'Union européenne, constituées d'Etats qui ont choisi librement, en vertu des traités qui les ont instituées, d'exercer en commun certaines de leurs compétences ». Le Conseil constitutionnel déduit de cette disposition que : « la transposition en droit interne d'une directive communautaire résulte d'une exigence constitutionnelle »[280]. Il en va de même

[280] Voir notamment la décision n° 2004-496 DC du 10 juin 2004, « Loi pour la confiance dans l'économie numérique ».

pour une loi ayant pour objet d'adapter le droit interne à un règlement de l'Union européenne[281].

1.3. CADRE CONVENTIONNEL

L'article 48 (2) du règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) n° 1060/2009, (UE) n° 648/2012, (UE) n° 600/2014, (UE) n° 909/2014 et (UE) 2016/1011, ci-après « règlement DORA », prévoit 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 qui leur sont nécessaires pour s'acquitter des missions qui leur incombent en vertu du présent règlement, 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.

Par ailleurs, l'article 49 (2) du règlement DORA prévoit que les autorités compétentes doivent coopérer étroitement entre elles et échangent des informations afin de s'acquitter de leurs missions, notamment leurs pouvoirs de surveillance, d'enquête et de sanction prévus à l'article 50 du règlement DORA.

1.4. ÉLEMENTS DE DROIT COMPARE

Les autres Etats membres de l'Union européenne devront prévoir dans leurs droits internes des obligations de coopération entre les différentes autorités compétentes pour assurer la mise en œuvre du règlement DORA.

2. NECESSITE DE LEGIFERER ET OBJECTIFS POURSUIVIS

2.1. NECESSITE DE LEGIFERER

La nécessité de légiférer provient ici de l'obligation constitutionnelle de transposition en droit interne d'une directive imposée par l'article 88-1 de la Constitution qui dispose que « [l]a République participe à l'Union européenne ». Cette obligation a d'ailleurs été rappelée par le Conseil constitutionnel dans le considérant 7 de sa décision n° 2004-496 DC du 10 juin 2004 : « Considérant qu'aux termes de l'article 88-1 de la Constitution […] ; qu'ainsi, la transposition en droit interne d'une directive communautaire résulte d'une exigence

[281] Voir par exemple la décision n° 2018-765, « Loi relative à la protection des données personnelles », considérant 3.

constitutionnelle à laquelle il ne pourrait être fait obstacle qu'en raison d'une disposition expresse contraire de la Constitution ».

2.2. OBJECTIFS POURSUIVIS

Cet article modifie l'article L. 631-1 du code monétaire et financier afin de tirer les conséquences de la modification de l'article L. 521-10 du même code, relative aux prestataires de services de paiement assujettis à l'obligation de notification (cf. article 49 du présent projet de loi) et pour permettre aux autorités de supervision d'échanger des informations entre elles en matière de sécurité des systèmes d'information.

3. OPTIONS POSSIBLES ET DISPOSITIF RETENU

3.1. OPTIONS ENVISAGEES

Aucune autre option n'a été envisagée dans la mesure où cette disposition est commandée par une norme supérieure issue du droit de l'Union européenne.

3.2. OPTION RETENUE

La directive DORA ne prévoit que des modifications d'ordre technique des différentes directives sectorielles qui visent à assurer la cohérence avec les nouvelles exigences introduites par le règlement DORA. Dans un souci de cohérence en matière de partage d'informations, il a été décidé de modifier le quatrième alinéa du II de l'article L. 631-1 du code monétaire et financier afin de le mettre en adéquation avec le II de l'article L. 521-10 du même code (cf. article 49).

4. ANALYSE DES IMPACTS DES DISPOSITIONS ENVISAGEES

4.1. IMPACTS JURIDIQUES

4.1.1. Impacts sur l'ordre juridique interne

L'article L. 631-1 du code monétaire et financier est modifié.

4.1.2. Articulation avec le droit international et le droit de l'Union européenne

L'article 48 (2) du règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) n° 1060/2009, (UE) n° 648/2012, (UE) n° 600/2014, (UE) n° 909/2014 et (UE) 2016/1011, ci-après « règlement DORA », prévoit 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 qui leur sont nécessaires pour s'acquitter des missions qui leur incombent en vertu du présent règlement, 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.

Par ailleurs, l'article 49 (2) du règlement DORA prévoit que les autorités compétentes doivent coopérer étroitement entre elles et échangent des informations afin de s'acquitter de leurs missions, notamment leurs pouvoirs de surveillance, d'enquête et de sanction prévus à l'article 50 du règlement DORA.

4.2. IMPACTS ECONOMIQUES ET FINANCIERS

4.2.1. Impacts macroéconomiques

Néant.

4.2.2. Impacts sur les entreprises

Néant.

4.2.3. Impacts budgétaires

Néant.

4.3. IMPACTS SUR LES COLLECTIVITES TERRITORIALES

Néant. S'agissant d'articles relatifs au droit monétaire, bancaire et financier, le présent article est sans incidence sur le fonctionnement des collectivités territoriales.

4.4. IMPACTS SUR LES SERVICES ADMINISTRATIFS

L'ACPR et la Banque de France pourront échanger des informations avec l'AMF ou l'ANSSI dans le domaine de la sécurité des systèmes d'information.

4.5. IMPACTS SOCIAUX

4.5.1. Impacts sur la société

Néant.

4.5.2. Impacts sur les personnes en situation de handicap

Néant.

4.5.3. Impacts sur l'égalité entre les femmes et les hommes

Néant.

4.5.4. Impacts sur la jeunesse

Néant.

4.5.5. Impacts sur les professions réglementées

Néant.

4.6. IMPACTS SUR LES PARTICULIERS

Néant.

4.7. IMPACTS ENVIRONNEMENTAUX

Néant.

5. CONSULTATIONS ET MODALITES D'APPLICATION

5.1. CONSULTATIONS MENEES

En application de l'article L. 614-2 du code monétaire et financier, le Comité consultatif de la législation et de la réglementation financières (CCLRF) a été consulté a rendu un avis favorable le 23 mai 2024.

La rédaction proposée a en outre été envoyée pour information et sur base informelle aux services de l'Autorité de contrôle prudentiel et de résolution (ACPR).

5.2. MODALITES D'APPLICATION

5.2.1. Application dans le temps

Le présent article s'appliquera à compter du 17 janvier 2025 conformément à l'article 62 du présent projet de loi.

5.2.2. Application dans l'espace

La mesure s'applique à l'ensemble du territoire de la République.

Elle s'appliquera de plein droit aux collectivités territoriales régies par l'article 73 de la Constitution (Guadeloupe, Guyane, Martinique, La Réunion et Mayotte) et certaines des collectivités relevant de l'article 74 (Saint-Barthélemy, Saint Martin et Saint-Pierre-et-Miquelon).

L'article 4 de la loi du 29 juillet 1961, l'article 7 de la loi organique n° 2004-192 du 27 février 2004 portant statut d'autonomie de la Polynésie Française et l'article 6-2 de la loi n° 99-209 organique du 19 mars 1999 relative à la Nouvelle-Calédonie soumettent respectivement pour les Îles Wallis et Futuna, la Polynésie Française et la Nouvelle-Calédonie au principe de spécialité législative, les lois et règlements n'y étant applicables que sur mention expresse, dès lors qu'ils interviennent dans un domaine pour lequel l'Etat est compétent. En effet, l'Etat est compétent en matière bancaire et financière dans ces collectivités ultramarines régies par le principe de spécialité législative où toute création ou modification du code précité doit être rendue applicable par mention expresse.

Ainsi, l'article 56 du projet de loi rend applicables les présentes dispositions en Nouvelle-Calédonie, en Polynésie française et dans les îles Wallis et Futuna en modifiant les articles L. 783-13, L. 784-13 et L. 785-12 du code monétaire et financier.

Enfin, la modification de l'article L. 712-7 du code monétaire et financier réalisée par l'article 56 du projet de loi rend applicable le règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier à Saint-Pierre et Miquelon, en Nouvelle-Calédonie, en Polynésie française et dans les îles Wallis et Futuna qui sont des pays et territoires d'outre-mer où le droit de l'Union européenne ne s'applique pas.

Par coordination, l'article L. 781-1 est complété par les références au règlement (UE) 2022/2554 précité.

5.2.3. Textes d’application

Le présent article ne requiert aucune mesure d’application.

CHAPITRE II – DISPOSITIONS MODIFIANT LE CODE DES ASSURANCES

Article 57 – Nouvelles obligations pour les entreprises d'assurance et de réassurance en matière de gouvernance des risques liés à l'utilisation des systèmes d'information

1. ÉTAT DES LIEUX

1.1. CADRE GENERAL

Entrée en vigueur en 2016, 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 – dite « Solvabilité 2 » – a permis de refondre et d'harmoniser les règles applicables aux principaux organismes d'assurance et de réassurance afin de leur permettre d'exercer leur activité dans tout le marché intérieur. Dans un contexte marqué par la crise financière de 2008 et la nécessité d'une meilleure prise en compte de la diversité des risques par les acteurs assurantiels, la directive Solvabilité 2 a fait évoluer leurs obligations dans trois domaines qui constituent les trois piliers de la directive :

- **Pilier 1 : exigences quantitatives**. Les exigences en capital doivent mieux refléter les risques de marché liés à la politique d'investissement des organismes d'assurance ;
- **Pilier 2 : exigences qualitatives**. Les assureurs et réassureurs doivent désormais mettre en place un système de gouvernance et de gestion des risques robuste (développement de fonctions clés, « *fit and proper* », renforcement du contrôle interne, auto-évaluation des besoins de capital, principe de la « personne prudente ») ;
- **Pilier 3 : exigences renforcées en matière de transmission d'informations** à destination du superviseur (l'Autorité de contrôle prudentiel et de résolution – ACPR) et du grand public (renforcement de la transparence).

Les règles régissant le système de gouvernance (pilier 2) sont en particulier prévues aux articles 41 à 50 de la directive Solvabilité 2 et transposées en droit national par l'ordonnance n° 2015-378 du 2 avril 2015[282] de façon similaire dans les articles L.354-1 du code des

[282] 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).

assurances (CDA), L. 211-12 du code de la mutualité (CMUT) et L.931-7 du code de la sécurité sociale (CSS) qui concernent chacun des organismes distincts. Au moment de la transposition de la directive Solvabilité 2, il avait en effet été décidé de préserver au sein de chacun des trois codes (CDA, CMUT et CSS) les dispositions de gouvernance applicables respectivement aux entreprises d'assurance et de réassurance du CDA, aux mutuelles et unions du CMUT et aux institutions de prévoyance et unions du CSS plutôt que de procéder par renvoi vers le CDA – dans un souci de lisibilité et de cohérence des obligations de gouvernance incombant à chaque type d'organisme.

L'article L. 354-1 du CDA rend ainsi applicables aux entreprises d'assurance et de réassurance les exigences prévues par cette directive en matière de gouvernance. Il dispose que :

- Le système de gouvernance adopté par ces entreprises doit garantir une gestion saine et prudente de leur activité et faire l'objet d'un réexamen interne régulier ;
- Il comprend une structure organisationnelle transparente, avec une répartition claire et une séparation appropriée des responsabilités ainsi qu'avec un dispositif efficace de transmission des informations ;
- Il se décompose en deux activités – la gestion des risques et le contrôle interne – et en quatre fonctions clés, dotées d'une unique personne physique responsable – la fonction de gestion des risques, la fonction de vérification de la conformité, la fonction d'audit interne et la fonction actuarielle ;
- Il repose (i) sur des exigences de compétence et d'honorabilité, (ii) sur des politiques écrites relatives *a minima* à la gestion des risques, au contrôle interne, à l'audit interne et aux externalisations qu'elles mettent en œuvre et (iii) sur les principes de liberté d'organisation, de proportionnalité et de responsabilité des acteurs ;
- Les organismes concernés prennent les dispositions appropriées et proportionnées permettant d'assurer la continuité et la régularité de leurs activités.

1.2. CADRE CONSTITUTIONNEL

En vertu de l'article 88-1 de la Constitution qui dispose que « *[l]a République participe à l'Union européenne* », la transposition des directives européennes en droit national est une obligation constitutionnelle. Cette obligation a d'ailleurs été rappelée par le Conseil constitutionnel dans le considérant 7 de sa décision n° 2004-496 DC du 10 juin 2004 : « Considérant qu'aux termes de l'article 88-1 de la Constitution […] ; qu'ainsi, la transposition en droit interne d'une directive communautaire résulte d'une exigence constitutionnelle à laquelle il ne pourrait être fait obstacle qu'en raison d'une disposition expresse contraire de la Constitution ».

1.3. CADRE CONVENTIONNEL

Comme présenté ci-dessus, l'article L.354-1 du CDA rend applicables aux entreprises d'assurance et de réassurance les obligations en matière de gouvernance et de gestion des risques prévues au titre du pilier 2 de la directive « Solvabilité 2 ». Plus précisément, ces dispositions ont été transposées en droit interne par l'ordonnance n° 2015-378 du 2 avril 2015 susmentionnée.

La 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, ci-après « directive DORA », complète ces obligations de gouvernance et de gestion des risques prévues par la directive Solvabilité 2 en introduisant une nouvelle exigence de gestion des réseaux et des systèmes d'information conformément au 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, ci-après « règlement DORA ».

L'article L. 354-1 du CDA est ainsi modifié en conséquence. L'article L. 354-1 du CDA transpose ainsi les nouvelles obligations de gouvernance des risques liés à l'utilisation des technologies de l'information et de la communication (TIC) introduites par la directive DORA en application du règlement DORA. La date limite de la transposition est fixée au 17 janvier 2025.

1.4. ÉLEMENTS DE DROIT COMPARE

Sans objet.

2. NECESSITE DE LEGIFERER ET OBJECTIFS POURSUIVIS

2.1. NECESSITE DE LEGIFERER

La nécessité de légiférer provient ici de l'obligation constitutionnelle de transposition en droit interne d'une directive imposée par l'article 88-1 de la Constitution et rappelée par le Conseil constitutionnel dans sa décision n°2004-496 DC du 10 juin 2004 précitée.

Dans le cas d'espèce, l'article 2 paragraphe 1 de la directive (UE) 2022/2556 du 14 décembre 2022 (directive DORA) modifie l'article 41 paragraphe 4 de la directive Solvabilité 2 en introduisant une nouvelle obligation de mise en place et de gestion des réseaux et des

systèmes d'information pour les acteurs du secteur assurantiel conformément aux règles édictées par le règlement DORA. Cette obligation se matérialise notamment par :

- La mise en place d'un cadre de gouvernance et de contrôle interne qui garantit une gestion prudente des risques liés à l'utilisation d'outils numériques (définition de stratégies, de procédures, de protocoles et d'outils de sécurité de TIC qui visent à garantir la résilience de l'entité, désignation d'une fonction de contrôle responsable de la gestion et de la surveillance du risque lié aux TIC, audits internes réguliers, etc.) ;
- La mise en place de mécanismes de détection, classification et notification des incidents cybernétiques ;
- La réalisation de tests de résilience opérationnelle numérique ayant vocation à évaluer l'état de préparation des entités pour faire face aux risques liés aux TIC, à recenser les faiblesses et à mettre en œuvre des mesures correctives ;
- La mise en œuvre de garde-fous pour anticiper les risques liés au recours à des prestataires tiers de services TIC (définition par écrit des droits et obligations de l'entité financière et du prestataire tiers de services TIC, tenue d'un registre d'informations en rapport avec tous les accords contractuels portant sur l'utilisation de services TIC fournis par des prestataires tiers, communication régulière de ces informations aux autorités compétentes, etc.).

L'article 41 paragraphe 4 de la directive Solvabilité 2 ayant été transposé au sein de l'article L. 354-1 du code des assurances (CDA) et la transposition des directives étant une obligation constitutionnelle, il apparaît dès lors nécessaire de modifier cet article L. 354-1 en conséquence.

De la même façon, l'article 8 de la directive DORA modifie l'article 21 paragraphe 5 de la directive (UE) 2016/2341 (directive IRP) en introduisant une nouvelle obligation pour les institutions de retraite professionnelle de mise en place et de gestion des réseaux et des systèmes d'information conformément aux règles édictées par le règlement DORA. Cette obligation se matérialise de la même façon que celle incombant aux acteurs du secteur assurantiel évoqués ci-avant. Or, l'article L. 385-5 du CDA prévoit que le chapitre IV du titre V du livre III du même code – dont fait partie l'article L. 354-1 – s'applique aux fonds de retraite professionnelle supplémentaire. La modification de l'article L. 354-1 du CDA permet donc également de transposer la modification de l'article 21 paragraphe 5 de la directive IRP et ainsi de respecter l'obligation constitutionnelle de transposition des directives européennes en droit interne.

Indépendamment de la transposition *stricto sensu* de la directive DORA, il est utile de profiter de la modification de l'article L. 354-1 du CDA pour aligner sa rédaction avec celle des articles L. 211-12 du code de la mutualité (CMUT) et L. 931-7 du code de la sécurité sociale (CSS) – articles miroirs respectivement pour les mutuelles et les institutions de prévoyance, révisés également par le présent projet de loi. C'est ainsi qu'il est spécifié au sein de cet

article L. 354-1 que l'externalisation de certaines activités par l'assureur à un prestataire renvoie à une définition de l'externalisation prévue au 13° de l'article L. 310-3 du CDA.

2.2. OBJECTIFS POURSUIVIS

Cet article permet de transposer dans le CDA les nouvelles exigences pour les entreprises d'assurance et de réassurance ainsi que pour les institutions de retraite professionnelle de mise en place et de gestion des réseaux et des systèmes d'information conformément au règlement DORA, introduites par l'article 2 paragraphe 1 et l'article 8 de la directive DORA.

3. OPTIONS POSSIBLES ET DISPOSITIF RETENU

3.1. OPTIONS ENVISAGEES

Aucune autre option n'a été envisagée dans la mesure où cette disposition est commandée par une norme supérieure issue du droit de l'Union européenne.

3.2. OPTION RETENUE

La directive DORA ne prévoit que des modifications d'ordre technique des différentes directives sectorielles qui visent à assurer la cohérence avec les nouvelles exigences introduites par le règlement DORA. Dans un souci de simplicité et dans la mesure où la transposition de cette directive DORA est essentiellement d'ordre technique, il a été décidé de reproduire à l'identique dans l'article L. 354-1 du CDA la rédaction adoptée dans l'article 2 paragraphe 1 de la directive DORA, à savoir « et, en particulier, mettent en place et gèrent des réseaux et des systèmes d'information conformément au règlement (UE) 2022/2554 du Parlement européen et du Conseil ».

4. ANALYSE DES IMPACTS DES DISPOSITIONS ENVISAGEES

4.1. IMPACTS JURIDIQUES

4.1.1. Impacts sur l'ordre juridique interne

L'article L. 354-1 du code des assurances est modifié.

4.1.2. Articulation avec le droit international et le droit de l'Union européenne

Conformément à l'article 288 du traité sur le fonctionnement de l'Union européenne (TFUE), « [l]e règlement a une portée générale. Il est obligatoire dans tous ses éléments et il est directement applicable dans tout Etat membre. » En outre, ce même article du TFUE prévoit que « la directive lie tout Etat membre destinataire quant au résultat à atteindre, tout en laissant aux instances nationales la compétence quant à la forme et aux moyens ». Cela implique que tous les Etats membres de l'Union européenne seront tenus d'appliquer directement les dispositions du règlement DORA et de transposer dans leur ordre juridique interne les modifications induites par la directive DORA.

4.2. IMPACTS ECONOMIQUES ET FINANCIERS

4.2.1. Impacts macroéconomiques

Sans objet.

4.2.2. Impacts sur les entreprises

Les entreprises d'assurance et de réassurance et les institutions de retraite professionnelles vont devoir appliquer les nouvelles obligations prévues par le règlement DORA et la directive l'accompagnant en matière de résilience et de gouvernance cybernétique (cf. *supra*). Cela aura un impact en termes financiers, sur les effectifs et sur l'organisation interne de chaque organisme en fonction de sa taille et de son activité.

D'après les premières informations chiffrées communiquées par la fédération France Assureurs[283], les coûts induits par la mise en place du paquet DORA peuvent être évalués ainsi :

- En coûts de projet (« *built* ») : autour de 6 millions d'euros en 2024/2025 et jusqu'à 40 millions d'euros au total entre 2024 et 2027 ;
- En coûts opérationnels (« *run* ») : entre 700 000 euros et 3 millions d'euros.

En outre, des programmes DORA sont mis en place chez les assureurs et mobilisent beaucoup de ressources (RSSI/Juridiques/*Compliance*/Informatique/Gestion des risques). Certaines entités sont également accompagnées par des cabinets de conseil.

4.2.3. Impacts budgétaires

[283] La fédération France Assureurs regroupe l'ensemble des entreprises d'assurance et de réassurance qui opèrent en France et qui relèvent du Code des assurances. Cela recouvre 252 sociétés représentant plus de 99% de ce marché, d'après son site : Nos adhérents - France Assureurs (consulté le 17 mai 2024). La fédération fait partie des principaux interlocuteurs de l'Administration et des autorités politiques dans ses travaux sur le secteur de l'assurance.

Sans objet.

4.3. IMPACTS SUR LES COLLECTIVITES TERRITORIALES

Sans objet.

4.4. IMPACTS SUR LES SERVICES ADMINISTRATIFS

L'entrée en vigueur de ces nouvelles obligations en matière de cyber-résilience dans le secteur financier va avoir des répercussions sur l'activité de l'Autorité de contrôle prudentiel et de résolution (ACPR) et sur ses besoins en termes de ressources budgétaires et d'effectifs (impact sur les outils numériques utilisés et recrutement de profils spécialisés notamment).

A terme, cette réglementation va engendrer de nouvelles missions de surveillance des prestataires tiers de services de technologies de l'information et de la communication (TIC) et renforcer les tâches de surveillance sur les assujettis habituels (collecte de nouvelles données, production de nouveaux rapports, etc.).

L'ACPR ne dispose toutefois pas d'informations précises sur les impacts budgétaires et RH à ce stade. Elle est largement tributaire des orientations données par les trois autorités européennes de supervision et par la Banque centrale européenne, qui sont encore en cours de discussion.

Des groupes de travail ont été lancés pour préparer l'entrée en vigueur de cette nouvelle réglementation.

4.5. IMPACTS SOCIAUX

Sans objet.

4.5.1. Impacts sur la société

Sans objet.

4.5.2. Impacts sur les personnes en situation de handicap

Sans objet.

4.5.3. Impacts sur l'égalité entre les femmes et les hommes

Sans objet.

4.5.4. Impacts sur la jeunesse

Sans objet.

4.5.5. Impacts sur les professions réglementées

Les impacts financiers de DORA pour les cabinets de courtage assujettis vont dépendre du niveau de maturité de chacun.

Toutefois, d'après les premières estimations communiquées par le syndicat des courtiers d'assurance Planète CSCA, les coûts externes d'assistance sont évalués entre 20 000 et 50 000 euros par cabinet pour une première phase d'évaluation des besoins/initialisation de la procédure de mise en conformité. Cette évaluation n'inclut pas les coûts de mise en conformité totale sur tous les métiers concernés par DORA. D'après Planète CSCA, il est admis que ces derniers seront supérieurs à ceux engendrés par le RGPD car DORA concerne plus de métiers et de nouvelles procédures : plusieurs centaines de milliers d'euros au moins, en prenant en compte le principe de proportionnalité.

Planète CSCA considère également que DORA aura également indirectement un impact financier sur les cabinets de courtage non assujettis mais habilités par une entreprise d'assurance à souscrire/gérer un contrat d'assurance (courtiers délégataires). Les impacts financiers de DORA sur ce type d'acteurs sont en cours d'évaluation.

4.6. IMPACTS SUR LES PARTICULIERS

Les particuliers devraient indirectement tirer profit de ces nouvelles obligations imposées par le paquet DORA puisqu'elles visent à limiter le risque cyber des assureurs et les potentiels effets négatifs sur leur liquidité et leur solvabilité que des attaques cybernétiques systémiques pourraient générer.

4.7. IMPACTS ENVIRONNEMENTAUX

Sans objet.

5. CONSULTATIONS ET MODALITES D'APPLICATION

5.1. CONSULTATIONS MENEES

En application de l'article L. 614-2 du code monétaire et financier, le Comité consultatif de la législation et de la réglementation financières (CCLRF) a été consulté et a rendu un avis favorable le 23 mai 2024.

Elle a en outre été soumise pour avis respectivement aux services de l'Autorité de contrôle prudentiel et de résolution (ACPR), aux équipes de l'association France Assureurs, du Centre technique des institutions de prévoyance (CTIP) et de la Fédération nationale de la Mutualité française (FNMF).

5.2. MODALITES D'APPLICATION

5.2.1. Application dans le temps

Le présent article s'appliquera à compter du 17 janvier 2025 conformément à l'article 62 du présent projet de loi.

5.2.2. Application dans l'espace

Application de plein droit du présent article en Guadeloupe, Guyane, Martinique, à La Réunion et à Mayotte

Conformément au principe dit de « l'identité législative », les lois et règlements s'appliquent de plein droit, donc sans mention spéciale, dans les collectivités d'outre-mer de l'article 73 de la Constitution. Le régime législatif et réglementaire applicable en Guadeloupe, Guyane, Martinique, à La Réunion et, depuis le 31 mars 2011, à Mayotte est celui de la métropole.

Les collectivités régies par l'article 73 de la Constitution sont ainsi soumises de plein droit aux dispositions du code des assurances.

Application de plein droit du présent article à Saint-Barthélemy, Saint-Martin et Saint-Pierre-et-Miquelon

Les statuts de Saint-Barthélemy, Saint-Martin et de Saint-Pierre-et-Miquelon prévoient que la plupart des lois et règlements y sont applicables de plein droit :

- Le principe de l'applicabilité de plein droit des normes juridiques s'applique à Saint-Barthélemy et Saint-Martin, en vertu de leur statut défini par la loi organique du 21 février 2007. L'article LO 6213-1 du code général des collectivités territoriales (CGCT), issu de cette loi, énonce ainsi que : « Les dispositions législatives et réglementaires sont applicables de plein droit à Saint-Barthélemy, à l'exception de celles intervenant dans les matières qui relèvent […] de la compétence de la

collectivité [… l'assurance n'en fait pas partie]. » L'article LO 6313-1 du CGCT porte des dispositions identiques pour Saint-Martin ;

- A Saint-Pierre-et-Miquelon, les lois et règlements français sont applicables de plein droit en vertu de l'article LO 6413-1 du CGCT (« Les dispositions législatives et réglementaires sont applicables de plein droit à Saint-Pierre-et-Miquelon, à l'exception de celles qui interviennent […] dans l'une des matières relevant de la compétence de la collectivité [… l'assurance n'en fait pas partie]. »). Les collectivités de Saint-Barthélemy, Saint-Martin et de Saint-Pierre-et-Miquelon sont ainsi soumises de plein droit aux nouvelles dispositions du code des assurances.

Absence d'application du présent article en Polynésie française, en Nouvelle-Calédonie et dans les îles Wallis et Futuna

En application du principe dit de la « spécialité législative », les lois et règlements ne sont applicables en Polynésie française, en Nouvelle-Calédonie et au territoire des îles Wallis et Futuna que sur mention expresse du texte en cause ou s'ils y ont été rendus applicables par un texte spécial. Et ce uniquement dans les matières qui relèvent de la compétence de l'État.

Absence d'application du présent article en Polynésie française et en Nouvelle-Calédonie

En application de l'article 74 et du titre XIII de la Constitution, la loi organique n° 99-209 du 19 mars 1999 et la loi organique n° 2004-192 du 27 février 2004 ont doté, respectivement, la Nouvelle-Calédonie et la Polynésie française de compétences de droit commun, réservant à l'Etat des compétences d'attribution, limitativement énumérées, dans des domaines considérés comme régaliens. Ces deux collectivités disposent, depuis l'entrée en vigueur desdites lois organiques, la compétence en matière de droit des assurances : (i) l'article 22 de la loi organique du 19 mars 1999 donne expressément compétence à la Nouvelle-Calédonie en matière d'assurance, (ii) l'article 14 de la loi organique du 27 février 2004 ne cite pas l'assurance parmi les matières réservées à l'Etat.

Il résulte du cadre normatif rappelé ci-dessus que l'Etat ne peut désormais plus édicter de règles en matière de droit des assurances qui seraient applicables en Nouvelle-Calédonie ou en Polynésie française. Toutefois, en l'absence de texte abrogeant le code des assurances en Nouvelle-Calédonie et en Polynésie française, les dispositions de ce code expressément étendues à ces territoires, antérieurement à la dévolution de compétences, y demeurent applicables sous réserve que les autorités territoriales ne les aient ni modifiées ni abrogées (article 222 de la loi organique du 19 mars 1999 et article 11 de la loi organique du 27 février 2004). Ce corpus est constitué, dans sa partie législative, de normes antérieures à la loi n° 91-716 du 21 juillet 1991 portant diverses dispositions d'ordre économique et financier.

Le présent article ne prévoit aucune extension ou adaptation à la Nouvelle-Calédonie ou à la Polynésie française. De même, il ne modifie en aucun cas les dispositions du code des assurances antérieures à 1991, qui continuent à s'appliquer dans ces territoires.

Absence d'application du présent article dans les îles Wallis et Futuna

Dans le territoire des îles Wallis et Futuna, les lois et règlements s'appliquent uniquement sur mention expresse, en vertu de l'article 4 de la loi n°61-814 du 29 juillet 1961. L'applicabilité des textes est donc subordonnée à l'adoption d'une disposition expresse d'extension. La portée de ce principe s'étend à tous les textes y compris les textes modificatifs.

Le droit des assurances entre dans le champ des prérogatives de l'Etat. Le statut des îles Wallis et Futuna, fixé par la loi du 29 juillet 1961, lui confère des compétences d'attribution ne comprenant pas l'assurance. En outre, le code des assurances en vigueur sur ce territoire n'a pas été actualisé depuis 1991.

Le présent article ne prévoit aucune extension ou adaptation du nouveau régime de protection qu'il institue au territoire des îles Wallis et Futuna. De même, il ne modifie en aucun cas les dispositions du code des assurances antérieures à 1991, qui continuent à s'appliquer dans ce territoire.

5.2.3. Textes d'application

Le présent article ne requiert aucune mesure d'application.

Article 58 – Extension aux groupes d'assurance des nouvelles obligations de gouvernance des risques liés à l'utilisation des systèmes d'information

1. ÉTAT DES LIEUX

1.1. CADRE GENERAL

Entrée en vigueur en 2016, 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 – dite « Solvabilité 2 » – a permis de refondre et d'harmoniser les règles applicables aux principaux organismes d'assurance et de réassurance afin de leur permettre d'exercer leur activité dans tout le marché intérieur. Dans un contexte marqué par la crise financière de 2008 et la nécessité d'une meilleure prise en compte de la diversité des risques par les acteurs assurantiels, la directive Solvabilité 2 a fait évoluer leurs obligations dans trois domaines qui constituent les trois piliers de la directive :

- **Pilier 1 : exigences quantitatives**. Les exigences en capital doivent mieux refléter les risques de marché liés à la politique d'investissement des organismes d'assurance ;
- **Pilier 2 : exigences qualitatives**. Les assureurs et réassureurs doivent désormais mettre en place un système de gouvernance et de gestion des risques robuste (développement de fonctions clés, « *fit and proper* », renforcement du contrôle interne, auto-évaluation des besoins de capital, principe de la « personne prudente ») ;
- **Pilier 3 : exigences renforcées en matière de transmission d'informations** à destination du superviseur (l'Autorité de contrôle prudentiel et de résolution – ACPR) et du grand public (renforcement de la transparence).

Les règles régissant le système de gouvernance (pilier 2) sont en particulier prévues aux articles 41 à 50 de la directive Solvabilité 2 et transposées en droit national par l'ordonnance n° 2015-378 du 2 avril 2015[284] de façon similaire dans les articles L. 354-1 du code des assurances (CDA), L. 211-12 du code de la mutualité (CMUT) et L. 931-7 du code de la sécurité sociale (CSS) qui concernent chacun des organismes distincts. Au moment de la transposition de la directive Solvabilité 2, il avait en effet été décidé de préserver au sein de chacun des trois codes (CDA, CMUT et CSS) les dispositions de gouvernance applicables respectivement aux entreprises d'assurance et de réassurance du CDA, aux mutuelles et

[284] 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).

unions du CMUT et aux institutions de prévoyance et unions du CSS plutôt que de procéder par renvoi vers le CDA – dans un souci de lisibilité et de cohérence des obligations de gouvernance incombant à chaque type d'organisme.

L'article 246 de la directive Solvabilité 2 relatif au contrôle du système de gouvernance prévoit dans son paragraphe 1 que « *[l]es exigences prévues au titre I, du chapitre IV, section 2, s'appliquent* mutatis mutandis *au niveau du groupe* ». Cela signifie que les règles concernant les systèmes de gouvernance pour les entités individuelles prévues par les articles 41 à 50 susmentionnés s'appliquent de manière équivalente aux groupes. Plus précisément, les règles de gouvernance des groupes sont pour l'essentiel mises en œuvre par l'entreprise tête de groupe qui est soit une entreprise d'assurance ou de réassurance participante, soit une entreprise mère de type holding – c'est-à-dire une société de groupe d'assurance (SGA), une société de groupe d'assurance mutuelle (SGAM), une union mutualiste de groupe (UMG) ou une société de groupe assurantiel de protection sociale (SGAPS). Au total, les groupes soumis à la directive Solvabilité 2 sont soumis à certains principes généraux concernant leur système de gouvernance : une structure organisationnelle transparente adéquate, une répartition claire et une séparation appropriée des responsabilités, un dispositif efficace de transmission des informations. Ils doivent prendre des dispositions permettant d'assurer la continuité et la régularité dans l'exercice de leurs activités, notamment l'élaboration de plans d'urgence. En outre, ils doivent disposer d'un système de gouvernance leur permettant de « *déceler, mesurer, contrôler, gérer et déclarer, en permanence, les risques, aux niveaux individuel et agrégé, auxquels elles sont ou pourrait être exposés, ainsi que les interdépendances entre ces risques* » (article 44 de la directive Solvabilité 2 applicable aux groupes conformément à l'article 246 de cette même directive). La règlementation fixe enfin les domaines qui doivent impérativement être couverts par le système de gestion des risques et impose l'élaboration de politiques écrites dans ces domaines.

L'article 246 de la directive Solvabilité 2 a été transposé pour le volet législatif aux articles L. 356-18 et L. 356-19 du CDA. L'article L. 356-18 en particulier réplique pour les groupes les dispositions de l'article L. 354-1 du même code concernant les entités individuelles, à savoir :

- Le système de gouvernance adopté par les groupes doit garantir une gestion saine et prudente de leur activité et faire l'objet d'un réexamen interne régulier ;
- Il comprend une structure organisationnelle transparente, avec une répartition claire et une séparation appropriée des responsabilités ainsi qu'avec un dispositif efficace de transmission des informations ;
- Il se décompose en deux activités – la gestion des risques et le contrôle interne – et en quatre fonctions clés, dotées d'une unique personne physique responsable – la fonction de gestion des risques, la fonction de vérification de la conformité, la fonction d'audit interne et la fonction actuarielle ;

- Il repose (i) sur des exigences de compétence et d'honorabilité, (ii) sur des politiques écrites relatives *a minima* à la gestion des risques, au contrôle interne, à l'audit interne et aux externalisations qu'elles mettent en œuvre et (iii) sur les principes de liberté d'organisation, de proportionnalité et de responsabilité des acteurs ;
- Les organismes concernés prennent les dispositions appropriées et proportionnées permettant d'assurer la continuité et la régularité de leurs activités.

L'article L. 356-18 du CDA prévoit en sus que la direction des groupes en question est assurée par deux personnes au moins.

1.2. CADRE CONSTITUTIONNEL

En vertu de l'article 88-1 de la Constitution qui dispose que « *[l]a République participe à l'Union européenne* », la transposition des directives européennes en droit national est une obligation constitutionnelle. Cette obligation a d'ailleurs été rappelée par le Conseil constitutionnel dans le considérant 7 de sa décision n° 2004-496 DC du 10 juin 2004 : « *Considérant qu'aux termes de l'article 88-1 de la Constitution […] ; qu'ainsi, la transposition en droit interne d'une directive communautaire résulte d'une exigence constitutionnelle à laquelle il ne pourrait être fait obstacle qu'en raison d'une disposition expresse contraire de la Constitution* ».

1.3. CADRE CONVENTIONNEL

Comme présenté ci-dessus, l'article L. 356-18 du CDA rend applicables aux groupes assurantiels les obligations en matière de gouvernance et de gestion des risques prévues au titre du pilier 2 de la directive Solvabilité 2. Plus précisément, ces dispositions ont été transposées en droit interne par l'ordonnance n° 2015-378 du 2 avril 2015 de transposition de la directive susmentionnée.

La 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, ci-après « directive DORA », complète ces obligations de gouvernance et de gestion des risques prévues par la directive Solvabilité 2 en introduisant une nouvelle exigence de gestion des réseaux et des systèmes d'information conformément au 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, ci-après « règlement DORA ». Ces nouvelles obligations de gouvernance des risques numériques s'appliquent également aux groupes d'assurance.

L'article L. 356-18 du CDA est ainsi modifié en conséquence. L'article L. 356-18 du CDA transpose ainsi les nouvelles obligations de gouvernance des risques liés à l'utilisation des technologies de l'information et de la communication (TIC) introduites par la directive DORA en application du règlement DORA. La date limite de la transposition est fixée au 17 janvier 2025.

1.4. ÉLEMENTS DE DROIT COMPARE

Sans objet.

2. NECESSITE DE LEGIFERER ET OBJECTIFS POURSUIVIS

2.1. NECESSITE DE LEGIFERER

La nécessité de légiférer provient ici de l'obligation constitutionnelle de transposition en droit interne d'une directive imposée par l'article 88-1 de la Constitution et rappelée par le Conseil constitutionnel dans sa décision n° 2004-496 DC du 10 juin 2004 précitée.

Dans le cas d'espèce, l'article 2 paragraphe 1 de la directive DORA modifie l'article 41 paragraphe 4 de la directive Solvabilité 2 en introduisant une nouvelle obligation pour les acteurs du secteur assurantiel de mise en place et de gestion des réseaux et des systèmes d'information conformément aux règles édictées par le règlement DORA. Cette obligation se matérialise notamment par :

- La mise en place d'un cadre de gouvernance et de contrôle interne qui garantit une gestion prudente des risques liés à l'utilisation d'outils numériques (définition de stratégies, de procédures, de protocoles et d'outils de sécurité de TIC qui visent à garantir la résilience de l'entité, désignation d'une fonction de contrôle responsable de la gestion et de la surveillance du risque lié aux TIC, audits internes réguliers, etc.) ;
- La mise en place de mécanismes de détection, classification et notification des incidents cybernétiques ;
- La réalisation de tests de résilience opérationnelle numérique ayant vocation à évaluer l'état de préparation des entités pour faire face aux risques liés aux TIC, à recenser les faiblesses et à mettre en œuvre des mesures correctives ;
- La mise en œuvre de garde-fous pour anticiper les risques liés au recours à des prestataires tiers de services TIC (définition par écrit des droits et obligations de l'entité financière et du prestataire tiers de services TIC, tenue d'un registre d'informations en rapport avec tous les accords contractuels portant sur l'utilisation de services TIC fournis par des prestataires tiers, communication régulière de ces informations aux autorités compétentes, etc.).

Conformément à l'article 246 paragraphe 1 de la directive Solvabilité 2, les modifications de l'article 41 de cette même directive relatives à la gouvernance numérique des entités individuelles s'appliquent également à la gouvernance numérique des groupes. L'article 246 ayant notamment été transposé au sein de l'article L. 356-18 du CDA qui réplique pour les groupes les dispositions de l'article L. 354-1 du même code et la transposition des directives étant une obligation constitutionnelle, il apparaît dès lors nécessaire de modifier cet article L. 356-18 en conséquence et dans les mêmes termes que l'article L. 354-1 (cf. article 57 du présent projet de loi).

2.2. OBJECTIFS POURSUIVIS

Cet article permet de transposer dans le CDA les nouvelles exigences pour les groupes d'assurance et de réassurance de mise en place et de gestion des réseaux et des systèmes d'information conformément au règlement DORA, introduites par jeu de renvoi par l'article 2 paragraphe 1 de la directive DORA.

3. OPTIONS POSSIBLES ET DISPOSITIF RETENU

3.1. OPTIONS ENVISAGEES

Aucune autre option n'a été envisagée dans la mesure où cette disposition est commandée par une norme supérieure issue du droit de l'Union européenne.

3.2. OPTION RETENUE

La directive DORA ne prévoit que des modifications d'ordre technique des différentes directives sectorielles qui visent à assurer la cohérence avec les nouvelles exigences introduites par le règlement DORA. Dans un souci de simplicité et dans la mesure où la transposition de cette directive DORA est d'ordre essentiellement technique, il a été décidé de reproduire à l'identique dans l'article L. 356-18 du CDA la rédaction adoptée dans l'article 2 paragraphe 1 de la directive DORA et reproduite à l'identique dans l'article L. 354-1 du CDA modifié, à savoir « et, en particulier, mettent en place et gèrent des réseaux et des systèmes d'information conformément au règlement (UE) 2022/2554 du Parlement européen et du Conseil ».

Indépendamment de la transposition de la directive DORA *stricto sensu* et suivant la modification de l'article L. 354-1 du CDA entreprise à l'article 57 du présent projet de loi, il est également précisé au sein de l'article L. 356-18 du CDA que l'externalisation de certaines activités par le groupe à un prestataire renvoie à une définition de l'externalisation prévue au 13° de l'article L. 310-3 du CDA.

4. ANALYSE DES IMPACTS DES DISPOSITIONS ENVISAGEES

4.1. IMPACTS JURIDIQUES

4.1.1. Impacts sur l'ordre juridique interne

L'article L. 356-18 du code des assurances est modifié.

4.1.2. Articulation avec le droit international et le droit de l'Union européenne

Conformément à l'article 288 du traité sur le fonctionnement de l'Union européenne (TFUE), « la directive lie tout Etat membre destinataire quant au résultat à atteindre, tout en laissant aux instances nationales la compétence quant à la forme et aux moyens », les autres Etats membres seront eux aussi tenus de mettre en application ces modifications induites par la directive DORA.

4.2. IMPACTS ECONOMIQUES ET FINANCIERS

4.2.1. Impacts macroéconomiques

Sans objet.

4.2.2. Impacts sur les entreprises

Les groupes d'assurance et de réassurance vont devoir appliquer les nouvelles obligations prévues par le règlement DORA et la directive l'accompagnant en matière de résilience et de gouvernance cybernétique (cf. *supra*). Cela aura un impact en termes financiers, sur les effectifs et sur l'organisation interne de chaque organisme en fonction de sa taille et de son activité. Ces groupes devront en outre veiller à la cohérence des systèmes de gouvernance de chacun des organismes les composant.

D'après les premières informations chiffrées communiquées par la fédération France Assureurs, les coûts induits par la mise en place du paquet DORA peuvent être évalués ainsi :

- En coûts de projet (« *built* ») : autour de 6 millions d'euros en 2024/2025 et jusqu'à 40 millions d'euros au total entre 2024 et 2027 ;
- En coûts opérationnels (« *run* ») : entre 700 000 euros et 3 millions d'euros.

En outre, des programmes DORA sont mis en place chez les assureurs et mobilisent beaucoup de ressources (RSSI/Juridiques/*Compliance*/Informatique/Gestion des risques). Certaines entités sont également accompagnées par des cabinets de conseil.

4.2.3. Impacts budgétaires

Sans objet.

4.3. IMPACTS SUR LES COLLECTIVITES TERRITORIALES

Sans objet.

4.4. IMPACTS SUR LES SERVICES ADMINISTRATIFS

L'entrée en vigueur de ces nouvelles obligations en matière de cyber-résilience dans le secteur financier va avoir des répercussions sur l'activité de l'Autorité de contrôle prudentiel et de résolution (ACPR) et sur ses besoins en termes de ressources budgétaires et d'effectifs (impact sur les outils numériques utilisés et recrutement de profils spécialisés notamment).

A terme, cette réglementation va engendrer de nouvelles missions de surveillance des prestataires tiers de services de technologies de l'information et de la communication (TIC) et renforcer les tâches de surveillance sur les assujettis habituels (collecte de nouvelles données, production de nouveaux rapports, etc.).

L'ACPR ne dispose toutefois pas d'informations précises sur les impacts budgétaires et RH à ce stade. Elle est largement tributaire des orientations données par les trois autorités européennes de supervision et par la Banque centrale européenne, qui sont encore en cours de discussion.

Des groupes de travail ont été lancés pour préparer l'entrée en vigueur de cette nouvelle réglementation.

4.5. IMPACTS SOCIAUX

4.5.1. Impacts sur la société

Sans objet.

4.5.2. Impacts sur les personnes en situation de handicap

Sans objet.

4.5.3. Impacts sur l'égalité entre les femmes et les hommes

Sans objet.

4.5.4. Impacts sur la jeunesse

Sans objet.

4.5.5. Impacts sur les professions réglementées

Les impacts financiers de DORA pour les cabinets de courtage assujettis vont dépendre du niveau de maturité de chacun.

Toutefois, d'après les premières estimations communiquées par le syndicat des courtiers d'assurance Planète CSCA, les coûts externes d'assistance sont évalués entre 20 000 et 50 000 euros par cabinet pour une première phase d'évaluation des besoins/initialisation de la procédure de mise en conformité. Cette évaluation n'inclut pas les coûts de mise en conformité totale sur tous les métiers concernés par DORA. D'après Planète CSCA, il est admis que ces derniers seront supérieurs à ceux engendrés par le RGPD car DORA concerne plus de métiers et de nouvelles procédures : plusieurs centaines de milliers d'euros au moins, en prenant en compte le principe de proportionnalité.

Planète CSCA considère également que DORA aura également indirectement un impact financier sur les cabinets de courtage non assujettis mais habilités par une entreprise d'assurance à souscrire/gérer un contrat d'assurance (courtiers délégataires). Les impacts financiers de DORA sur ce type d'acteurs sont en cours d'évaluation.

4.6. IMPACTS SUR LES PARTICULIERS

Les particuliers devraient indirectement tirer profit de ces nouvelles obligations imposées par le paquet DORA puisqu'elles visent à limiter le risque cyber des assureurs et les potentiels effets négatifs sur leur liquidité et leur solvabilité que des attaques cybernétiques systémiques pourraient générer.

4.7. IMPACTS ENVIRONNEMENTAUX

Sans objet.

5. CONSULTATIONS ET MODALITES D'APPLICATION

5.1. CONSULTATIONS MENEES

En application de l'article L. 614-2 du code monétaire et financier, le Comité consultatif de la législation et de la réglementation financières (CCLRF) a été consulté et a rendu un avis favorable le 23 mai 2024.

Elle a en outre été soumise pour avis respectivement aux services de l'Autorité de contrôle prudentiel et de résolution (ACPR), aux équipes de l'association France Assureurs, du Centre technique des institutions de prévoyance (CTIP) et de la Fédération nationale de la Mutualité française (FNMF).

5.2. MODALITES D'APPLICATION

5.2.1. Application dans le temps

Le présent article s'appliquera à compter du 17 janvier 2025 conformément à l'article 62 du présent projet de loi.

5.2.2. Application dans l'espace

Application de plein droit du présent article en Guadeloupe, Guyane, Martinique, à La Réunion et à Mayotte

Conformément au principe dit de « l'identité législative », les lois et règlements s'appliquent de plein droit, donc sans mention spéciale, dans les collectivités d'outre-mer de l'article 73 de la Constitution. Le régime législatif et réglementaire applicable en Guadeloupe, Guyane, Martinique, à La Réunion et, depuis le 31 mars 2011, à Mayotte est celui de la métropole.

Les collectivités régies par l'article 73 de la Constitution sont ainsi soumises de plein droit aux dispositions du code des assurances.

Application de plein droit du présent article à Saint-Barthélemy, Saint-Martin et Saint-Pierre-et-Miquelon

Les statuts de Saint-Barthélemy, Saint-Martin et de Saint-Pierre-et-Miquelon prévoient que la plupart des lois et règlements y sont applicables de plein droit :

- Le principe de l'applicabilité de plein droit des normes juridiques s'applique à Saint-Barthélemy et Saint-Martin, en vertu de leur statut défini par la loi organique du 21 février 2007. L'article LO 6213-1 du code général des collectivités territoriales (CGCT), issu de cette loi, énonce ainsi que : « Les dispositions législatives et réglementaires sont applicables de plein droit à Saint-Barthélemy, à l'exception de celles intervenant dans les matières qui relèvent […] de la compétence de la

collectivité [… l'assurance n'en fait pas partie]. » L'article LO 6313-1 du CGCT porte des dispositions identiques pour Saint-Martin ;

- A Saint-Pierre-et-Miquelon, les lois et règlements français sont applicables de plein droit en vertu de l'article LO 6413-1 du CGCT (« Les dispositions législatives et réglementaires sont applicables de plein droit à Saint-Pierre-et-Miquelon, à l'exception de celles qui interviennent […] dans l'une des matières relevant de la compétence de la collectivité [… l'assurance n'en fait pas partie]. »). Les collectivités de Saint-Barthélemy, Saint-Martin et de Saint-Pierre-et-Miquelon sont ainsi soumises de plein droit aux nouvelles dispositions du code des assurances.

Absence d'application du présent article en Polynésie française, en Nouvelle-Calédonie et dans les îles Wallis et Futuna

En application du principe dit de la « spécialité législative », les lois et règlements ne sont applicables en Polynésie française, en Nouvelle-Calédonie et au territoire des îles Wallis et Futuna que sur mention expresse du texte en cause ou s'ils y ont été rendus applicables par un texte spécial. Et ce uniquement dans les matières qui relèvent de la compétence de l'État.

Absence d'application du présent article en Polynésie française et en Nouvelle-Calédonie

En application de l'article 74 et du titre XIII de la Constitution, la loi organique n° 99-209 du 19 mars 1999 et la loi organique n° 2004-192 du 27 février 2004 ont doté, respectivement, la Nouvelle-Calédonie et la Polynésie française de compétences de droit commun, réservant à l'Etat des compétences d'attribution, limitativement énumérées, dans des domaines considérés comme régaliens. Ces deux collectivités disposent, depuis l'entrée en vigueur desdites lois organiques, la compétence en matière de droit des assurances : (i) l'article 22 de la loi organique du 19 mars 1999 donne expressément compétence à la Nouvelle-Calédonie en matière d'assurance, (ii) l'article 14 de la loi organique du 27 février 2004 ne cite pas l'assurance parmi les matières réservées à l'Etat.

Il résulte du cadre normatif rappelé ci-dessus que l'Etat ne peut désormais plus édicter de règles en matière de droit des assurances qui seraient applicables en Nouvelle-Calédonie ou en Polynésie française. Toutefois, en l'absence de texte abrogeant le code des assurances en Nouvelle-Calédonie et en Polynésie française, les dispositions de ce code expressément étendues à ces territoires, antérieurement à la dévolution de compétences, y demeurent applicables sous réserve que les autorités territoriales ne les aient ni modifiées ni abrogées (article 222 de la loi organique du 19 mars 1999 et article 11 de la loi organique du 27 février 2004). Ce corpus est constitué, dans sa partie législative, de normes antérieures à la loi n° 91-716 du 21 juillet 1991 portant diverses dispositions d'ordre économique et financier.

Le présent article ne prévoit aucune extension ou adaptation à la Nouvelle-Calédonie ou à la Polynésie française. De même, il ne modifie en aucun cas les dispositions du code des assurances antérieures à 1991, qui continuent à s'appliquer dans ces territoires.

<u>Absence d'application du présent article dans les îles Wallis et Futuna</u>

Dans le territoire des îles Wallis et Futuna, les lois et règlements s'appliquent uniquement sur mention expresse, en vertu de l'article 4 de la loi n° 61-814 du 29 juillet 1961. L'applicabilité des textes est donc subordonnée à l'adoption d'une disposition expresse d'extension. La portée de ce principe s'étend à tous les textes y compris les textes modificatifs.

Le droit des assurances entre dans le champ des prérogatives de l'Etat. Le statut des îles Wallis et Futuna, fixé par la loi du 29 juillet 1961, lui confère des compétences d'attribution ne comprenant pas l'assurance. En outre, le code des assurances en vigueur sur ce territoire n'a pas été actualisé depuis 1991.

Le présent article ne prévoit aucune extension ou adaptation du nouveau régime de protection qu'il institue au territoire des îles Wallis et Futuna. De même, il ne modifie en aucun cas les dispositions du code des assurances antérieures à 1991, qui continuent à s'appliquer dans ce territoire.

5.2.3. Textes d'application

Le présent article ne requiert aucune mesure d'application.

CHAPITRE III – DISPOSITIONS MODIFIANT LE CODE DE LA MUTUALITE

Article 59 – Nouvelles obligations pour les unions et mutuelles du code de la mutualité en matière de gouvernance des risques liés à l'utilisation des systèmes d'information

1. ÉTAT DES LIEUX

1.1. CADRE GENERAL

Entrée en vigueur en 2016, 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 – dite « Solvabilité 2 » – a permis de refondre et d'harmoniser les règles applicables aux principaux organismes d'assurance et de réassurance afin de leur permettre d'exercer leur activité dans tout le marché intérieur. Dans un contexte marqué par la crise financière de 2008 et la nécessité d'une meilleure prise en compte de la diversité des risques par les acteurs assurantiels, la directive Solvabilité 2 a fait évoluer leurs obligations dans trois domaines qui constituent les trois piliers de la directive :

- **Pilier 1 : exigences quantitatives**. Les exigences en capital doivent mieux refléter les risques de marché liés à la politique d'investissement des organismes d'assurance ;
- **Pilier 2 : exigences qualitatives**. Les assureurs et réassureurs doivent désormais mettre en place un système de gouvernance et de gestion des risques robuste (développement de fonctions clés, « *fit and proper* », renforcement du contrôle interne, auto-évaluation des besoins de capital, principe de la « personne prudente ») ;
- **Pilier 3 : exigences renforcées en matière de transmission d'informations** à destination du superviseur (l'Autorité de contrôle prudentiel et de résolution – ACPR) et du grand public (renforcement de la transparence).

Les règles régissant le système de gouvernance (pilier 2) sont en particulier prévues aux articles 41 à 50 de la directive Solvabilité 2 et transposées en droit national par l'ordonnance n° 2015-378 du 2 avril 2015 de façon similaire dans les articles L. 354-1 du code des assurances (CDA), L. 211-12 du code de la mutualité (CMUT) et L. 931-7 du code de la sécurité sociale (CSS) qui concernent chacun des organismes distincts. Au moment de la transposition de la directive Solvabilité 2, il avait en effet été décidé de préserver au sein de chacun des trois codes (CDA, CMUT et CSS) les dispositions de gouvernance applicables

respectivement aux entreprises d'assurance et de réassurance du CDA, aux mutuelles et unions du CMUT et aux institutions de prévoyance et unions du CSS plutôt que de procéder par renvoi vers le CDA – dans un souci de lisibilité et de cohérence des obligations de gouvernance incombant à chaque type d'organisme.

L'article L. 211-12 du CMUT rend ainsi applicables aux mutuelles et unions de ce code les exigences prévues par cette directive en matière de gouvernance. Il dispose que :

- Le système de gouvernance adopté par ces entreprises doit garantir une gestion saine et prudente de leur activité et faire l'objet d'un réexamen interne régulier ;
- Il comprend une structure organisationnelle transparente, avec une répartition claire et une séparation appropriée des responsabilités ainsi qu'avec un dispositif efficace de transmission des informations ;
- Il se décompose en deux activités – la gestion des risques et le contrôle interne – et en quatre fonctions clés, dotées d'une unique personne physique responsable – la fonction de gestion des risques, la fonction de vérification de la conformité, la fonction d'audit interne et la fonction actuarielle ;
- Il repose (i) sur des exigences de compétence et d'honorabilité, (ii) sur des politiques écrites relatives *a minima* à la gestion des risques, au contrôle interne, à l'audit interne et aux externalisations qu'elles mettent en œuvre et (iii) sur les principes de liberté d'organisation, de proportionnalité et de responsabilité des acteurs ;
- Les organismes concernés prennent les dispositions appropriées et proportionnées permettant d'assurer la continuité et la régularité de leurs activités.

1.2. CADRE CONSTITUTIONNEL

En vertu de l'article 88-1 de la Constitution qui dispose que « *[l]a République participe à l'Union européenne* », la transposition des directives européennes en droit national est une obligation constitutionnelle. Cette obligation a d'ailleurs été rappelée par le Conseil constitutionnel dans le considérant 7 de sa décision n° 2004-496 DC du 10 juin 2004 : « *Considérant qu'aux termes de l'article 88-1 de la Constitution […] ; qu'ainsi, la transposition en droit interne d'une directive communautaire résulte d'une exigence constitutionnelle à laquelle il ne pourrait être fait obstacle qu'en raison d'une disposition expresse contraire de la Constitution* ».

1.3. CADRE CONVENTIONNEL

Comme présenté ci-dessus, l'article L. 211-12 du CMUT rend applicables aux mutuelles et unions de ce code les obligations en matière de gouvernance et de gestion des risques prévues

au titre du pilier 2 de la directive « Solvabilité 2 ». Plus précisément, ces dispositions ont été transposées en droit interne par l'ordonnance n° 2015-378 du 2 avril 2015 susmentionnée.

La 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, ci-après « directive DORA », complète ces obligations de gouvernance et de gestion des risques prévues par la directive Solvabilité 2 en introduisant une nouvelle exigence de gestion des réseaux et des systèmes d'information conformément au 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, ci-après « règlement DORA ».

L'article L. 211-12 du CMUT est ainsi modifié en conséquence. L'article L. 211-12 du CMUT transpose ainsi les nouvelles obligations de gouvernance des risques liés à l'utilisation des technologies de l'information et de la communication (TIC) introduites par la directive DORA en application du règlement DORA. La date limite de la transposition est fixée au 17 janvier 2025.

1.4. ÉLEMENTS DE DROIT COMPARE

Sans objet.

2. NECESSITE DE LEGIFERER ET OBJECTIFS POURSUIVIS

2.1. NECESSITE DE LEGIFERER

La nécessité de légiférer provient ici de l'obligation constitutionnelle de transposition en droit interne d'une directive imposée par l'article 88-1 de la Constitution et rappelée par le Conseil constitutionnel dans le considérant 7 de sa décision n° 2004-496 DC du 10 juin 2004 précitée.

Dans le cas d'espèce, l'article 2 paragraphe 1 de la directive DORA modifie l'article 41 paragraphe 4 de la directive Solvabilité 2 en introduisant une nouvelle obligation pour les acteurs du secteur assurantiel de mise en place et de gestion des réseaux et des systèmes d'information conformément aux règles édictées par le règlement DORA. Cette obligation se matérialise notamment par :

- La mise en place d'un cadre de gouvernance et de contrôle interne qui garantit une gestion prudente des risques liés à l'utilisation d'outils numériques (définition de stratégies, de procédures, de protocoles et d'outils de sécurité de TIC qui visent à

garantir la résilience de l'entité, désignation d'une fonction de contrôle responsable de la gestion et de la surveillance du risque lié aux TIC, audits internes réguliers, etc.) ;
- La mise en place de mécanismes de détection, classification et notification des incidents cybernétiques ;
- La réalisation de tests de résilience opérationnelle numérique ayant vocation à évaluer l'état de préparation des entités pour faire face aux risques liés aux TIC, à recenser les faiblesses et à mettre en œuvre des mesures correctives ;
- La mise en œuvre de garde-fous pour anticiper les risques liés au recours à des prestataires tiers de services TIC (définition par écrit des droits et obligations de l'entité financière et du prestataire tiers de services TIC, tenue d'un registre d'informations en rapport avec tous les accords contractuels portant sur l'utilisation de services TIC fournis par des prestataires tiers, communication régulière de ces informations aux autorités compétentes, etc.).

L'article 41 paragraphe 4 de la directive Solvabilité 2 ayant été transposé au sein de l'article L. 211-12 du CMUT de la même façon que l'article L. 354-1 du CDA et la transposition des directives étant une obligation constitutionnelle, il apparaît dès lors nécessaire de modifier cet article L. 211-12 du CMUT en conséquence et dans les mêmes termes que l'article L. 354-1 du CDA (cf. article 57 du présent projet de loi).

2.2. OBJECTIFS POURSUIVIS

Cet article permet de transposer dans le CMUT les nouvelles exigences pour les mutuelles et unions de ce code de mise en place et de gestion des réseaux et des systèmes d'information conformément au règlement DORA, introduites par l'article 2 paragraphe 1 de la directive DORA.

3. OPTIONS POSSIBLES ET DISPOSITIF RETENU

3.1. OPTIONS ENVISAGEES

Aucune autre option n'a été envisagée dans la mesure où cette disposition est commandée par une norme supérieure issue du droit de l'Union européenne.

3.2. OPTION RETENUE

La directive DORA ne prévoit que des modifications d'ordre technique des différentes directives sectorielles qui visent à assurer la cohérence avec les nouvelles exigences introduites par le règlement DORA. Dans un souci de simplicité et dans la mesure où la

transposition de cette directive DORA est d'ordre essentiellement technique, il a été décidé de reproduire à l'identique dans l'article L. 211-12 du CMUT la rédaction adoptée dans l'article 2 paragraphe 1 de la directive DORA et reproduite à l'identique dans l'article L. 354-1 du CDA modifié, à savoir « et, en particulier, mettent en place et gèrent des réseaux et des systèmes d'information conformément au règlement (UE) 2022/2554 du Parlement européen et du Conseil ».

4. ANALYSE DES IMPACTS DES DISPOSITIONS ENVISAGEES

4.1. IMPACTS JURIDIQUES

4.1.1. Impacts sur l'ordre juridique interne

L'article L. 211-12 du CMUT est modifié.

4.1.2. Articulation avec le droit international et le droit de l'Union européenne

Conformément à l'article 288 du traité sur le fonctionnement de l'Union européenne (TFUE), « [l]e règlement a une portée générale. Il est obligatoire dans tous ses éléments et il est directement applicable dans tout Etat membre. » En outre, ce même article du TFUE prévoit que « la directive lie tout Etat membre destinataire quant au résultat à atteindre, tout en laissant aux instances nationales la compétence quant à la forme et aux moyens ». Cela implique que tous les Etats membres de l'Union européenne seront tenus d'appliquer directement les dispositions du règlement DORA et de transposer dans leur ordre juridique interne les modifications induites par la directive DORA.

4.2. IMPACTS ECONOMIQUES ET FINANCIERS

4.2.1. Impacts macroéconomiques

Sans objet.

4.2.2. Impacts sur les entreprises

Les mutuelles et unions du CMUT vont devoir appliquer les nouvelles obligations prévues par le règlement DORA et la directive l'accompagnant en matière de résilience et de gouvernance cybernétique. Cela aura un impact en termes financiers, sur les effectifs et sur l'organisation interne de chaque organisme en fonction de sa taille et de son activité.

4.2.3. Impacts budgétaires

Sans objet.

4.3. IMPACTS SUR LES COLLECTIVITES TERRITORIALES

Sans objet.

4.4. IMPACTS SUR LES SERVICES ADMINISTRATIFS

L'entrée en vigueur de ces nouvelles obligations en matière de cyber-résilience dans le secteur financier va avoir des répercussions sur l'activité de l'Autorité de contrôle prudentiel et de résolution (ACPR) et sur ses besoins en termes de ressources budgétaires et d'effectifs (impact sur les outils numériques utilisés et recrutement de profils spécialisés notamment).

A terme, cette réglementation va engendrer de nouvelles missions de surveillance des prestataires tiers de services de technologies de l'information et de la communication (TIC) et renforcer les tâches de surveillance sur les assujettis habituels (collecte de nouvelles données, production de nouveaux rapports, etc.).

L'ACPR ne dispose toutefois pas d'informations précises sur les impacts budgétaires et RH à ce stade. Elle est largement tributaire des orientations données par les trois autorités européennes de supervision et par la Banque centrale européenne, qui sont encore en cours de discussion.

Des groupes de travail ont été lancés pour préparer l'entrée en vigueur de cette nouvelle réglementation.

4.5. IMPACTS SOCIAUX

4.5.1. Impacts sur la société

Sans objet.

4.5.2. Impacts sur les personnes en situation de handicap

Sans objet.

4.5.3. Impacts sur l'égalité entre les femmes et les hommes

Sans objet.

4.5.4. Impacts sur la jeunesse

Sans objet.

4.5.5. Impacts sur les professions réglementées

Les impacts financiers de DORA pour les cabinets de courtage assujettis vont dépendre du niveau de maturité de chacun.

Toutefois, d'après les premières estimations communiquées par le syndicat des courtiers d'assurance Planète CSCA, les coûts externes d'assistance sont évalués entre 20 000 et 50 000 euros par cabinet pour une première phase d'évaluation des besoins/initialisation de la procédure de mise en conformité. Cette évaluation n'inclut pas les coûts de mise en conformité totale sur tous les métiers concernés par DORA. D'après Planète CSCA, il est admis que ces derniers seront supérieurs à ceux engendrés par le RGPD car DORA concerne plus de métiers et de nouvelles procédures : plusieurs centaines de milliers d'euros au moins, en prenant en compte le principe de proportionnalité.

Planète CSCA considère également que DORA aura également indirectement un impact financier sur les cabinets de courtage non assujettis mais habilités par une entreprise d'assurance à souscrire/gérer un contrat d'assurance (courtiers délégataires). Les impacts financiers de DORA sur ce type d'acteurs sont en cours d'évaluation.

4.6. IMPACTS SUR LES PARTICULIERS

Les particuliers devraient indirectement tirer profit de ces nouvelles obligations imposées par le paquet DORA puisqu'elles visent à limiter le risque cyber des assureurs et les potentiels effets négatifs sur leur liquidité et leur solvabilité que des attaques cybernétiques systémiques pourraient générer.

4.7. IMPACTS ENVIRONNEMENTAUX

Sans objet.

5. CONSULTATIONS ET MODALITES D'APPLICATION

5.1. CONSULTATIONS MENEES

En application de l'article L. 614-2 du code monétaire et financier, le Comité consultatif de la législation et de la réglementation financières (CCLRF) a été consulté et a rendu un avis favorable le 23 mai 2024.

Elle a en outre été soumise pour avis respectivement aux services de l'Autorité de contrôle prudentiel et de résolution (ACPR), aux équipes de l'association France Assureurs, du Centre technique des institutions de prévoyance (CTIP) et de la Fédération nationale de la Mutualité française (FNMF).

5.2. MODALITES D'APPLICATION

5.2.1. Application dans le temps

Le présent article s'appliquera à compter du 17 janvier 2025 conformément à l'article 62 du présent projet de loi.

5.2.2. Application dans l'espace

Application de plein droit du présent article en Guadeloupe, Guyane, Martinique, à La Réunion et à Mayotte

Conformément au principe dit de « l'identité législative », les lois et règlements s'appliquent de plein droit, donc sans mention spéciale, dans les collectivités d'outre-mer de l'article 73 de la Constitution. Le régime législatif et réglementaire applicable en Guadeloupe, Guyane, Martinique, à La Réunion et, depuis le 31 mars 2011, à Mayotte est celui de la métropole.

Les collectivités régies par l'article 73 de la Constitution sont ainsi soumises de plein droit aux dispositions du code de la mutualité.

Application de plein droit du présent article à Saint-Barthélemy, Saint-Martin et Saint-Pierre-et-Miquelon

Les statuts de Saint-Barthélemy, Saint-Martin et de Saint-Pierre-et-Miquelon prévoient que la plupart des lois et règlements y sont applicables de plein droit :

- Le principe de l'applicabilité de plein droit des normes juridiques s'applique à Saint-Barthélemy et Saint-Martin, en vertu de leur statut défini par la loi organique du 21 février 2007. L'article LO 6213-1 du code général des collectivités territoriales (CGCT), issu de cette loi, énonce ainsi que : « Les dispositions législatives et réglementaires sont applicables de plein droit à Saint-Barthélemy, à l'exception de celles intervenant dans les matières qui relèvent […] de la compétence de la

collectivité [… le droit de la mutualité n'en fait pas partie]. » L'article LO 6313-1 du CGCT porte des dispositions identiques pour Saint-Martin ;

- A Saint-Pierre-et-Miquelon, les lois et règlements français sont applicables de plein droit en vertu de l'article LO 6413-1 du CGCT (« Les dispositions législatives et réglementaires sont applicables de plein droit à Saint-Pierre-et-Miquelon, à l'exception de celles qui interviennent […] dans l'une des matières relevant de la compétence de la collectivité [… le droit de la mutualité n'en fait pas partie]. »). Les collectivités de Saint-Barthélemy, Saint-Martin et de Saint-Pierre-et-Miquelon sont ainsi soumises de plein droit aux nouvelles dispositions du code de la mutualité.

Absence d'application du présent article en Polynésie française, en Nouvelle-Calédonie et dans les îles Wallis et Futuna

En application du principe dit de la « spécialité législative », les lois et règlements ne sont applicables en Polynésie française, en Nouvelle-Calédonie et au territoire des îles Wallis et Futuna que sur mention expresse du texte en cause ou s'ils y ont été rendus applicables par un texte spécial. Et ce uniquement dans les matières qui relèvent de la compétence de l'État. Or, le droit de la mutualité relève des compétences propres des collectivités du Pacifique.

5.2.3. Textes d'application

Le présent article ne requiert aucune mesure d'application.

Article 60 – Suppression de dispositions redondantes dans le code de la mutualité

1. ÉTAT DES LIEUX

1.1. CADRE GENERAL

Entrée en vigueur en 2016, 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 – dite « Solvabilité 2 » – a permis de refondre et d'harmoniser les règles applicables aux principaux organismes d'assurance et de réassurance afin de leur permettre d'exercer leur activité dans tout le marché intérieur. Dans un contexte marqué par la crise financière de 2008 et la nécessité d'une meilleure prise en compte de la diversité des risques par les acteurs assurantiels, la directive Solvabilité 2 a fait évoluer leurs obligations dans trois domaines qui constituent les trois piliers de la directive :

- **Pilier 1 : exigences quantitatives**. Les exigences en capital doivent mieux refléter les risques de marché liés à la politique d'investissement des organismes d'assurance ;
- **Pilier 2 : exigences qualitatives**. Les assureurs et réassureurs doivent désormais mettre en place un système de gouvernance et de gestion des risques robuste (développement de fonctions clés, « *fit and proper* », renforcement du contrôle interne, auto-évaluation des besoins de capital, principe de la « personne prudente ») ;
- **Pilier 3 : exigences renforcées en matière de transmission d'informations** à destination du superviseur (l'Autorité de contrôle prudentiel et de résolution – ACPR) et du grand public (renforcement de la transparence).

Les règles régissant le système de gouvernance (pilier 2) sont en particulier prévues aux articles 41 à 50 de la directive Solvabilité 2 et transposées en droit national par l'ordonnance n° 2015-378 du 2 avril 2015[285] de façon similaire dans les articles L. 354-1 du code des assurances (CDA), L. 211-12 du code de la mutualité (CMUT) et L. 931-7 du code de la sécurité sociale (CSS) qui concernent chacun des organismes distincts. Au moment de la transposition de la directive Solvabilité 2, il avait en effet été décidé de préserver au sein de chacun des trois codes (CDA, CMUT et CSS) les dispositions de gouvernance applicables respectivement aux entreprises d'assurance et de réassurance du CDA, aux mutuelles et unions du CMUT et aux institutions de prévoyance et unions du CSS plutôt que de procéder

[285] 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).

par renvoi vers le CDA – dans un souci de lisibilité et de cohérence des obligations de gouvernance incombant à chaque type d'organisme.

L'article L. 211-12 du CMUT, en particulier, rend ainsi applicables aux mutuelles et unions de ce code les exigences prévues par cette directive en matière de gouvernance. Il dispose que :

- Le système de gouvernance adopté par ces entreprises doit garantir une gestion saine et prudente de leur activité et faire l'objet d'un réexamen interne régulier ;
- Il comprend une structure organisationnelle transparente, avec une répartition claire et une séparation appropriée des responsabilités ainsi qu'avec un dispositif efficace de transmission des informations ;
- Il se décompose en deux activités – la gestion des risques et le contrôle interne – et en quatre fonctions clés, dotées d'une unique personne physique responsable – la fonction de gestion des risques, la fonction de vérification de la conformité, la fonction d'audit interne et la fonction actuarielle ;
- Il repose (i) sur des exigences de compétence et d'honorabilité, (ii) sur des politiques écrites relatives *a minima* à la gestion des risques, au contrôle interne, à l'audit interne et aux externalisations qu'elles mettent en œuvre et (iii) sur les principes de liberté d'organisation, de proportionnalité et de responsabilité des acteurs ;
- Les organismes concernés prennent les dispositions appropriées et proportionnées permettant d'assurer la continuité et la régularité de leurs activités.

En outre, l'ordonnance n° 2015-378 du 2 avril 2015 évoquée ci-dessus a également modifié l'article L.212-1 du CMUT qui prévoit notamment que « *[l]es dispositions du titre V du livre III […] du code des assurances sont applicables aux mutuelles et unions […]* », ce qui revient à dire que l'article L. 354-1 CDA est également applicable aux mutuelles et unions du CMUT. Autrement dit, à date, les mutuelles et unions du CMUT sont soumises à la fois aux dispositions de l'article L. 211-12 du CMUT et L. 354-1 du CDA – qui sont exactement les mêmes.

1.2. CADRE CONSTITUTIONNEL

En vertu de l'objectif à valeur constitutionnelle d'accessibilité et d'intelligibilité de la loi, cet article a simplement vocation à clarifier/simplifier une disposition du code de la mutualité et à rendre plus lisible le droit applicable.

1.3. CADRE CONVENTIONNEL

Comme présenté ci-dessus, par renvoi à l'article L. 354-1 du CDA, l'article L. 212-1 du CMUT rend applicables aux mutuelles et unions de ce code les obligations en matière de gouvernance et de gestion des risques prévues au titre du pilier 2 de la directive « Solvabilité 2 ». Plus précisément, ces dispositions ont été transposées en droit interne par l'ordonnance n° 2015-378 du 2 avril 2015 susmentionnée.

1.4. ÉLEMENTS DE DROIT COMPARE

Sans objet.

2. NECESSITE DE LEGIFERER ET OBJECTIFS POURSUIVIS

2.1. NECESSITE DE LEGIFERER

La nécessité de légiférer procède ici d'un souci de cohérence et de lisibilité du droit puisqu'il s'agit de supprimer les redondances entre l'article L. 211-12 et L. 212-1 du CMUT. En effet, comme évoqué ci-avant, l'article L. 212-1, dans sa version actuelle, prévoit que les mutuelles et unions du CMUT doivent appliquer les dispositions du titre V du livre III du CDA, notamment l'article L. 354-1. Dans la mesure où l'article L. 211-12 du CMUT reproduit les termes de l'article L. 354-1 du CDA et est modifié de la même façon dans le cadre de la transposition de la directive DORA, il n'apparaît dès lors pas nécessaire de maintenir dans l'article L. 212-1 du CMUT le renvoi vers cet article du CDA. C'est pourquoi le présent article exclut expressément l'application de l'article L. 354-1 du CDA pour les mutuelles et unions du CMUT.

La rédaction proposée est alignée avec celle de l'article L. 931-9 du CSS qui exclut lui-aussi l'application de l'article L. 354-1 du CDA pour les institutions de prévoyance et les unions du CSS – ces derniers étant déjà soumis aux obligations de l'article L. 931-7 du CSS qui répliquent celles de l'article L. 354-1 du CDA (cf. article 61 du présent projet de loi).

2.2. OBJECTIFS POURSUIVIS

Comme précisé ci-dessus, l'objectif du présent article est de rendre plus cohérentes et lisibles les dispositions applicables spécifiquement aux mutuelles et unions du CMUT, de la même façon que cela est fait dans le CSS. Plus largement, cela permet d'éviter de définir les exigences de gouvernance applicables aux mutuelles et unions du CMUT par renvoi vers le CDA, dans l'esprit de ce qui avait été fait au moment de la transposition de la directive Solvabilité 2 en 2015.

3. OPTIONS POSSIBLES ET DISPOSITIF RETENU

3.1. OPTIONS ENVISAGEES

Suivant le principe du parallélisme des formes, une disposition législative ne peut être modifiée que par une mesure de même niveau normatif. Ainsi, aucune autre option que le recours à la loi n'a été envisagée ici.

Le choix aurait pu être fait de ne pas modifier l'article L. 212-1 dont la rédaction ne pose pas de problème sur le fond. Il est néanmoins apparu préférable, par souci de cohérence, de dupliquer la rédaction d'une disposition analogue dans le code de la sécurité sociale.

3.2. OPTION RETENUE

En cohérence avec la rédaction adoptée au sein de l'article L. 931-9 du CSS modifié par l'ordonnance n° 2015-378 du 2 avril 2015 de transposition de la directive Solvabilité 2, il a été décidé d'insérer à la fin du deuxième alinéa de l'article L. 212-1 du CMUT les mots « , à l'exception de l'article L. 354-1 du code des assurances ».

4. ANALYSE DES IMPACTS DES DISPOSITIONS ENVISAGEES

4.1. IMPACTS JURIDIQUES

4.1.1. Impacts sur l'ordre juridique interne

L'article L. 212-1 du code de la mutualité est modifié.

4.1.2. Articulation avec le droit international et le droit de l'Union européenne

Sans objet.

4.2. IMPACTS ECONOMIQUES ET FINANCIERS

4.2.1. Impacts macroéconomiques

Sans objet.

4.2.2. Impacts sur les entreprises

Sans objet.

4.2.3. Impacts budgétaires

Sans objet.

4.3. IMPACTS SUR LES COLLECTIVITES TERRITORIALES

Sans objet.

4.4. IMPACTS SUR LES SERVICES ADMINISTRATIFS

Sans objet.

4.5. IMPACTS SOCIAUX

4.5.1. Impacts sur la société

Sans objet.

4.5.2. Impacts sur les personnes en situation de handicap

Sans objet.

4.5.3. Impacts sur l'égalité entre les femmes et les hommes

Sans objet.

4.5.4. Impacts sur la jeunesse

Sans objet.

4.5.5. Impacts sur les professions réglementées

Sans objet.

4.6. IMPACTS SUR LES PARTICULIERS

Sans objet.

4.7. IMPACTS ENVIRONNEMENTAUX

Sans objet.

5. CONSULTATIONS ET MODALITES D'APPLICATION

5.1. CONSULTATIONS MENEES

En application de l'article L. 614-2 du code monétaire et financier, le Comité consultatif de la législation et de la réglementation financières (CCLRF) a été consulté et a rendu un avis favorable le 23 mai 2024.

Elle a en outre été soumise pour avis respectivement aux services de l'Autorité de contrôle prudentiel et de résolution (ACPR), aux équipes de l'association France Assureurs, du Centre technique des institutions de prévoyance (CTIP) et de la Fédération nationale de la Mutualité française (FNMF).

5.2. MODALITES D'APPLICATION

5.2.1. Application dans le temps

Le présent article s'appliquera à compter du 17 janvier 2025 conformément à l'article 62 du présent projet de loi.

5.2.2. Application dans l'espace

Application de plein droit du présent article en Guadeloupe, Guyane, Martinique, à La Réunion et à Mayotte

Conformément au principe dit de « l'identité législative », les lois et règlements s'appliquent de plein droit, donc sans mention spéciale, dans les collectivités d'outre-mer de l'article 73 de la Constitution. Le régime législatif et réglementaire applicable en Guadeloupe, Guyane, Martinique, à La Réunion et, depuis le 31 mars 2011, à Mayotte est celui de la métropole.

Les collectivités régies par l'article 73 de la Constitution sont ainsi soumises de plein droit aux dispositions du code de la mutualité.

Application de plein droit du présent article à Saint-Barthélemy, Saint-Martin et Saint-Pierre-et-Miquelon

Les statuts de Saint-Barthélemy, Saint-Martin et de Saint-Pierre-et-Miquelon prévoient que la plupart des lois et règlements y sont applicables de plein droit :

- Le principe de l'applicabilité de plein droit des normes juridiques s'applique à Saint-Barthélemy et Saint-Martin, en vertu de leur statut défini par la loi organique du 21 février 2007. L'article LO 6213-1 du code général des collectivités territoriales (CGCT), issu de cette loi, énonce ainsi que : « Les dispositions législatives et réglementaires sont applicables de plein droit à Saint-Barthélemy, à l'exception de celles intervenant dans les matières qui relèvent […] de la compétence de la collectivité [… le droit de la mutualité n'en fait pas partie]. » L'article LO 6313-1 du CGCT porte des dispositions identiques pour Saint-Martin ;
- A Saint-Pierre-et-Miquelon, les lois et règlements français sont applicables de plein droit en vertu de l'article LO 6413-1 du CGCT (« Les dispositions législatives et réglementaires sont applicables de plein droit à Saint-Pierre-et-Miquelon, à l'exception de celles qui interviennent […] dans l'une des matières relevant de la compétence de la collectivité [… le droit de la mutualité n'en fait pas partie]. »). Les collectivités de Saint-Barthélemy, Saint-Martin et de Saint-Pierre-et-Miquelon sont ainsi soumises de plein droit aux nouvelles dispositions du code de la mutualité.

Absence d'application du présent article en Polynésie française, en Nouvelle-Calédonie et dans les îles Wallis et Futuna

En application du principe dit de la « spécialité législative », les lois et règlements ne sont applicables en Polynésie française, en Nouvelle-Calédonie et au territoire des îles Wallis et Futuna que sur mention expresse du texte en cause ou s'ils y ont été rendus applicables par un texte spécial. Et ce uniquement dans les matières qui relèvent de la compétence de l'État. Or, le droit de la mutualité relève des compétences propres des collectivités du Pacifique.

5.2.3. Textes d'application

Le présent article ne requiert aucune mesure d'application.

CHAPITRE IV – DISPOSITIONS MODIFIANT LE CODE DE LA SECURITE SOCIALE

Article 61 – Nouvelles obligations pour les institutions de prévoyance et unions du code de la sécurité sociale en matière de gouvernance des risques liés à l'utilisation des systèmes d'information

1. ÉTAT DES LIEUX

1.1. CADRE GENERAL

Entrée en vigueur en 2016, 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 – dite « Solvabilité 2 » – a permis de refondre et d'harmoniser les règles applicables aux principaux organismes d'assurance et de réassurance afin de leur permettre d'exercer leur activité dans tout le marché intérieur. Dans un contexte marqué par la crise financière de 2008 et la nécessité d'une meilleure prise en compte de la diversité des risques par les acteurs assurantiels, la directive Solvabilité 2 a fait évoluer leurs obligations dans trois domaines qui constituent les trois piliers de la directive :

- **Pilier 1 : exigences quantitatives**. Les exigences en capital doivent mieux refléter les risques de marché liés à la politique d'investissement des organismes d'assurance ;
- **Pilier 2 : exigences qualitatives**. Les assureurs et réassureurs doivent désormais mettre en place un système de gouvernance et de gestion des risques robuste (développement de fonctions clés, « *fit and proper* », renforcement du contrôle interne, auto-évaluation des besoins de capital, principe de la « personne prudente ») ;
- **Pilier 3 : exigences renforcées en matière de transmission d'informations** à destination du superviseur (l'Autorité de contrôle prudentiel et de résolution – ACPR) et du grand public (renforcement de la transparence).

Les règles régissant le système de gouvernance (pilier 2) sont en particulier prévues aux articles 41 à 50 de la directive Solvabilité 2 et transposées en droit national par l'ordonnance n° 2015-378 du 2 avril 2015 de façon similaire dans les articles L. 354-1 du code des assurances (CDA), L. 211-12 du code de la mutualité (CMUT) et L. 931-7 du code de la sécurité sociale (CSS) qui concernent chacun des organismes distincts. Au moment de la transposition de la directive Solvabilité 2, il avait en effet été décidé de préserver au sein de

chacun des trois codes (CDA, CMUT et CSS) les dispositions de gouvernance applicables respectivement aux entreprises d'assurance et de réassurance du CDA, aux mutuelles et unions du CMUT et aux institutions de prévoyance et unions du CSS plutôt que de procéder par renvoi vers le CDA – dans un souci de lisibilité et de cohérence des obligations de gouvernance incombant à chaque type d'organisme.

L'article L. 931-7 du CSS rend ainsi applicables aux institutions de prévoyance et unions de ce code les exigences prévues par cette directive en matière de gouvernance. Il dispose que :

- Le système de gouvernance adopté par ces entreprises doit garantir une gestion saine et prudente de leur activité et faire l'objet d'un réexamen interne régulier ;
- Il comprend une structure organisationnelle transparente, avec une répartition claire et une séparation appropriée des responsabilités ainsi qu'avec un dispositif efficace de transmission des informations ;
- Il se décompose en deux activités – la gestion des risques et le contrôle interne – et en quatre fonctions clés, dotées d'une unique personne physique responsable – la fonction de gestion des risques, la fonction de vérification de la conformité, la fonction d'audit interne et la fonction actuarielle ;
- Il repose (i) sur des exigences de compétence et d'honorabilité, (ii) sur des politiques écrites relatives *a minima* à la gestion des risques, au contrôle interne, à l'audit interne et aux externalisations qu'elles mettent en œuvre et (iii) sur les principes de liberté d'organisation, de proportionnalité et de responsabilité des acteurs ;
- Les organismes concernés prennent les dispositions appropriées et proportionnées permettant d'assurer la continuité et la régularité de leurs activités.

1.2. CADRE CONSTITUTIONNEL

En vertu de l'article 88-1 de la Constitution qui dispose que « [l]a République participe à l'Union européenne », la transposition des directives européennes en droit national est une obligation constitutionnelle. Cette obligation a d'ailleurs été rappelée par le Conseil constitutionnel dans le considérant 7 de sa décision n° 2004-496 DC du 10 juin 2004 : « Considérant qu'aux termes de l'article 88-1 de la Constitution […] ; qu'ainsi, la transposition en droit interne d'une directive communautaire résulte d'une exigence constitutionnelle à laquelle il ne pourrait être fait obstacle qu'en raison d'une disposition expresse contraire de la Constitution ».

1.3. CADRE CONVENTIONNEL

Comme présenté ci-dessus, l'article L. 931-7 du CSS rend applicables aux institutions de prévoyance et unions de ce code les obligations en matière de gouvernance et de gestion des risques prévues au titre du pilier 2 de la directive « Solvabilité 2 ». Plus précisément, ces dispositions ont été transposées en droit interne par l'ordonnance n° 2015-378 du 2 avril 2015 susmentionnée.

La 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, ci-après « directive DORA », complète ces obligations de gouvernance et de gestion des risques prévues par la directive Solvabilité 2 en introduisant une nouvelle exigence de gestion des réseaux et des systèmes d'information conformément au 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, ci-après « règlement DORA ».

L'article L. 931-7 du CSS est ainsi modifié en conséquence. L'article L. 931-7 du CSS transpose ainsi les nouvelles obligations de gouvernance des risques liés à l'utilisation des technologies de l'information et de la communication (TIC) introduites par la directive DORA en application du règlement DORA. La date limite de la transposition est fixée au 17 janvier 2025.

1.4. ÉLEMENTS DE DROIT COMPARE

Sans objet.

2. NECESSITE DE LEGIFERER ET OBJECTIFS POURSUIVIS

2.1. NECESSITE DE LEGIFERER

La nécessité de légiférer provient ici de l'obligation constitutionnelle de transposition en droit interne d'une directive imposée par l'article 88-1 de la Constitution et rappelée par le Conseil constitutionnel dans le considérant 7 de sa décision n° 2004-496 DC du 10 juin 2004 précitée.

Dans le cas d'espèce, l'article 2 paragraphe 1 de la directive DORA modifie l'article 41 paragraphe 4 de la directive Solvabilité 2 en introduisant une nouvelle obligation pour les acteurs du secteur assurantiel de mise en place et de gestion des réseaux et des systèmes d'information conformément aux règles édictées par le règlement DORA. Cette obligation se matérialise notamment par :

- La mise en place d'un cadre de gouvernance et de contrôle interne qui garantit une gestion prudente des risques liés à l'utilisation d'outils numériques (définition de stratégies, de procédures, de protocoles et d'outils de sécurité de TIC qui visent à garantir la résilience de l'entité, désignation d'une fonction de contrôle responsable de la gestion et de la surveillance du risque lié aux TIC, audits internes réguliers, etc.) ;
- La mise en place de mécanismes de détection, classification et notification des incidents cybernétiques ;
- La réalisation de tests de résilience opérationnelle numérique ayant vocation à évaluer l'état de préparation des entités pour faire face aux risques liés aux TIC, à recenser les faiblesses et à mettre en œuvre des mesures correctives ;
- La mise en œuvre de garde-fous pour anticiper les risques liés au recours à des prestataires tiers de services TIC (définition par écrit des droits et obligations de l'entité financière et du prestataire tiers de services TIC, tenue d'un registre d'informations en rapport avec tous les accords contractuels portant sur l'utilisation de services TIC fournis par des prestataires tiers, communication régulière de ces informations aux autorités compétentes, etc.).

D'une part, l'article 41 paragraphe 4 de la directive Solvabilité 2 ayant été transposé au sein de l'article L. 931-7 du CSS de la même façon que l'article L. 354-1 du CDA et que l'article L. 211-12 du CMUT et, d'autre part, la transposition des directives étant une obligation constitutionnelle, il apparaît dès lors nécessaire de modifier cet article L. 931-7 du CSS en conséquence et dans les mêmes termes que les articles L. 354-1 du CDA et L. 211-12 du CMUT (cf. articles 57 et 59 du présent projet de loi).

2.2. OBJECTIFS POURSUIVIS

Cet article permet de transposer dans le CSS les nouvelles exigences pour les instituts de prévoyance et unions de ce code de mise en place et de gestion des réseaux et des systèmes d'information conformément au règlement DORA, introduites par l'article 2 paragraphe 1 de la directive DORA.

3. OPTIONS POSSIBLES ET DISPOSITIF RETENU

3.1. OPTIONS ENVISAGEES

Aucune autre option n'a été envisagée dans la mesure où cette disposition est commandée par une norme supérieure issue du droit de l'Union européenne.

3.2. OPTION RETENUE

La directive DORA ne prévoit que des modifications d'ordre technique des différentes directives sectorielles qui visent à assurer la cohérence avec les nouvelles exigences introduites par le règlement DORA. Dans un souci de simplicité et dans la mesure où la transposition de cette directive DORA est d'ordre essentiellement technique, il a été décidé de reproduire à l'identique dans l'article L. 931-7 du CSS la rédaction adoptée dans l'article 2 paragraphe 1 de la directive DORA et reproduite à l'identique dans les articles L.354-1 du CDA et L.211-12 du CMUT modifiés, à savoir « *et, en particulier, mettent en place et gèrent des réseaux et des systèmes d'information conformément au règlement (UE) 2022/2554 du Parlement européen et du Conseil* ».

4. ANALYSE DES IMPACTS DES DISPOSITIONS ENVISAGEES

4.1. IMPACTS JURIDIQUES

4.1.1. Impacts sur l'ordre juridique interne

L'article L. 931-7 du code de la sécurité sociale est modifié.

4.1.2. Articulation avec le droit international et le droit de l'Union européenne

Conformément à l'article 288 du traité sur le fonctionnement de l'Union européenne (TFUE), « [l]e règlement a une portée générale. Il est obligatoire dans tous ses éléments et il est directement applicable dans tout Etat membre. » En outre, ce même article du TFUE prévoit que « la directive lie tout Etat membre destinataire quant au résultat à atteindre, tout en laissant aux instances nationales la compétence quant à la forme et aux moyens ». Cela implique que tous les Etats membres de l'Union européenne seront tenus d'appliquer directement les dispositions du règlement DORA et de transposer dans leur ordre juridique interne les modifications induites par la directive DORA.

4.2. IMPACTS ECONOMIQUES ET FINANCIERS

4.2.1. Impacts macroéconomiques

Sans objet.

4.2.2. Impacts sur les entreprises

Les institutions de prévoyance et unions du CSS vont devoir appliquer les nouvelles obligations prévues par le règlement DORA et la directive l'accompagnant en matière de résilience et de gouvernance cybernétique. Cela aura un impact en termes financiers, sur les

effectifs et sur l'organisation interne de chaque organisme en fonction de sa taille et de son activité.

4.2.3. Impacts budgétaires

Sans objet.

4.3. IMPACTS SUR LES COLLECTIVITES TERRITORIALES

Sans objet

4.4. IMPACTS SUR LES SERVICES ADMINISTRATIFS

L'entrée en vigueur de ces nouvelles obligations en matière de cyber-résilience dans le secteur financier va avoir des répercussions sur l'activité de l'Autorité de contrôle prudentiel et de résolution (ACPR) et sur ses besoins en termes de ressources budgétaires et d'effectifs (impact sur les outils numériques utilisés et recrutement de profils spécialisés notamment).

A terme, cette réglementation va engendrer de nouvelles missions de surveillance des prestataires tiers de services de technologies de l'information et de la communication (TIC) et renforcer les tâches de surveillance sur les assujettis habituels (collecte de nouvelles données, production de nouveaux rapports, etc.).

L'ACPR ne dispose toutefois pas d'informations précises sur les impacts budgétaires et RH à ce stade. Elle est largement tributaire des orientations données par les trois autorités européennes de supervision et par la Banque centrale européenne, qui sont encore en cours de discussion.

Des groupes de travail ont été lancés pour préparer l'entrée en vigueur de cette nouvelle réglementation.

4.5. IMPACTS SOCIAUX

4.5.1. Impacts sur la société

Sans objet.

4.5.2. Impacts sur les personnes en situation de handicap

Sans objet.

4.5.3. Impacts sur l'égalité entre les femmes et les hommes

Sans objet.

4.5.4. Impacts sur la jeunesse

Sans objet.

4.5.5. Impacts sur les professions réglementées

Les impacts financiers de DORA pour les cabinets de courtage assujettis vont dépendre du niveau de maturité de chacun.

Toutefois, d'après les premières estimations communiquées par le syndicat des courtiers d'assurance Planète CSCA, les coûts externes d'assistance sont évalués entre 20 000 et 50 000 euros par cabinet pour une première phase d'évaluation des besoins/initialisation de la procédure de mise en conformité. Cette évaluation n'inclut pas les coûts de mise en conformité totale sur tous les métiers concernés par DORA. D'après Planète CSCA, il est admis que ces derniers seront supérieurs à ceux engendrés par le RGPD car DORA concerne plus de métiers et de nouvelles procédures : plusieurs centaines de milliers d'euros au moins, en prenant en compte le principe de proportionnalité.

Planète CSCA considère également que DORA aura également indirectement un impact financier sur les cabinets de courtage non assujettis mais habilités par une entreprise d'assurance à souscrire/gérer un contrat d'assurance (courtiers délégataires). Les impacts financiers de DORA sur ce type d'acteurs sont en cours d'évaluation.

4.6. IMPACTS SUR LES PARTICULIERS

Les particuliers devraient indirectement tirer profit de ces nouvelles obligations imposées par le paquet DORA puisqu'elles visent à limiter le risque cyber des assureurs et les potentiels effets négatifs sur leur liquidité et leur solvabilité que des attaques cybernétiques systémiques pourraient générer.

4.7. IMPACTS ENVIRONNEMENTAUX

Sans objet.

5. CONSULTATIONS ET MODALITES D'APPLICATION

5.1. CONSULTATIONS MENEES

En application de l'article L. 614-2 du code monétaire et financier, le Comité consultatif de la législation et de la réglementation financières (CCLRF) a été consulté et a rendu un avis favorable le 23 mai 2024.

Elle a en outre été soumise pour avis respectivement aux services de l'Autorité de contrôle prudentiel et de résolution (ACPR), aux équipes de l'association France Assureurs, du Centre technique des institutions de prévoyance (CTIP) et de la Fédération nationale de la Mutualité française (FNMF).

5.2. MODALITES D'APPLICATION

5.2.1. Application dans le temps

Le présent article s'appliquera à compter du 17 janvier 2025 conformément à l'article 62 du présent projet de loi.

5.2.2. Application dans l'espace

Application de plein droit du présent article en Guadeloupe, Guyane, Martinique et à La Réunion

Conformément au principe dit de « l'identité législative », les lois et règlements s'appliquent de plein droit, donc sans mention spéciale, dans les collectivités d'outre-mer de l'article 73 de la Constitution. Le régime législatif et réglementaire applicable en Guadeloupe, Guyane, Martinique, à La Réunion et, depuis le 31 mars 2011, à Mayotte est celui de la métropole.

Les collectivités régies par l'article 73 de la Constitution, sauf Mayotte, sont ainsi soumises de plein droit aux dispositions du code de la sécurité sociale.

Application de plein droit du présent article à Saint-Barthélemy et à Saint-Martin

Les statuts de Saint-Barthélemy, Saint-Martin prévoient que la plupart des lois et règlements y sont applicables de plein droit :

Le principe de l'applicabilité de plein droit des normes juridiques s'applique à Saint-Barthélemy et Saint-Martin, en vertu de leur statut défini par la loi organique du 21 février 2007. L'article LO 6213-1 du code général des collectivités territoriales (CGCT), issu de cette loi, énonce ainsi que : « *Les dispositions législatives et réglementaires sont applicables de plein droit à Saint-Barthélemy, à l'exception de celles intervenant dans les matières qui*

relèvent […] *de la compétence de la collectivité* [… le droit de la sécurité sociale n'en fait pas partie]. » L'article LO 6313-1 du CGCT porte des dispositions identiques pour Saint-Martin.

Absence d'application du présent article à Saint Pierre et Miquelon, en Polynésie française, en Nouvelle-Calédonie et dans les îles Wallis et Futuna

A Saint Pierre et Miquelon, les lois et règlements français sont applicables de plein droit en vertu de l'article LO 6413-1 du CGCT (« Les dispositions législatives et réglementaires sont applicables de plein droit à Saint-Pierre-et-Miquelon, à l'exception de celles qui interviennent […] dans l'une des matières relevant de la compétence de la collectivité […Or, le droit de la sécurité sociale en fait partie]. »).

En application du principe dit de la « spécialité législative », les lois et règlements ne sont applicables en Polynésie française, en Nouvelle-Calédonie et au territoire des îles Wallis et Futuna que sur mention expresse du texte en cause ou s'ils y ont été rendus applicables par un texte spécial. Et ce uniquement dans les matières qui relèvent de la compétence de l'État. Or, le droit de la mutualité relève des compétences propres des collectivités du Pacifique.

5.2.3. Textes d'application

Le présent article ne requiert aucune mesure d'application.

CHAPITRE V – DISPOSITIONS FINALES

Article 62 – Dates d'application des dispositions du titre III sur la résilience opérationnelle numérique du secteur financier

1. ÉTAT DES LIEUX

1.1. CADRE GENERAL

L'article 9(1) de la 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, ci-après « directive DORA » prévoit que les Etats membres adoptent les dispositions nécessaires pour se conformer et appliquent ces dispositions au plus tard le 17 janvier 2025. L'ensemble des dispositions visant à la mise en conformité de la France à l'égard de la directive DORA sont inclues au sein du titre III du projet de loi. Afin de d'assurer que la directive DORA soit transposée conformément au calendrier exigé par cette même directive, le présent article prévoit que les dispositions du titre III du projet de loi relatif à la résilience opérationnelle numérique entrent en application à compter du 17 janvier 2025.

Toutefois, le présent article prévoit également une date d'entrée en application différée de certaines dispositions du projet de loi. Les articles 46, 47 et 54 de ce projet de loi sont applicables aux sociétés de financement. Les sociétés de financement sont des établissements financiers, autres que des établissements de crédit, qui effectuent à titre de profession habituelle et pour leur propre compte des opérations de crédit dans les conditions et limites définies par leur agrément. Elles ne collectent pas de dépôts et fonds remboursables du public. L'article L. 511-41 et suivants du code monétaire et financier ainsi que l'arrêté du 23 décembre 2013 relatif au régime prudentiel des sociétés de financement prévoient aujourd'hui que les sociétés de financement appliquent déjà les exigences prudentielles prévues au titre de la directive CRD et du règlement associé 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 dit « CRR » - à l'exception des dispositions relatives à au risque de liquidité et au ratio de levier prudentiel. L'application aux sociétés de financement d'exigences prudentielles comparables en termes de solidité à celles applicables aux établissements de crédit - et ce depuis l'entrée en application du cadre prudentiel européen en 2013 – a permis notamment à ces premières de bénéficier d'un traitement

prudentiel plus favorable, les expositions sur ces sociétés de financement pouvant être traitées comme des expositions sur les établissements de crédit au titre de la réglementation européenne (cf. article 119 du règlement CRR). C'est le maintien de cette comparabilité entre établissements de crédit et sociétés de financement qui est notamment recherché en appliquant aux sociétés de financement le cadre de DORA.

Afin d'accorder un délai de mise en œuvre supplémentaire pour les sociétés de financement considérées comme de taille petite et non-complexes et dont les moyens et ressources sont réputées moins importantes, l'article 62 de ce projet de loi introduit une entrée en application différée – repoussée d'un an au 17 janvier 2026 – des articles 46, 47 et 54 de ce projet de loi pour les sociétés de financement remplissant les conditions prévues au point 145 du paragraphe 1 de l'article 4 du règlement (UE) n° 575/2013 du Parlement européen et du Conseil dit « CRR » qui définit les établissements de petite taille et non complexe. Un établissement de petite taille et non complexe est un établissement qui remplit toutes les conditions suivantes :

a) il ne s'agit pas d'un établissement de grande taille;

b) la valeur totale de ses actifs sur base individuelle ou, le cas échéant, sur base consolidée conformément au présent règlement et à la directive 2013/36/UE est en moyenne égale ou inférieure à un seuil de cinq milliards d'euros sur la période de quatre ans qui précède immédiatement la période de déclaration annuelle en cours; les États membres peuvent abaisser ce seuil ;

c) 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 conformément à l'article 4 de la directive 2014/59/UE ;

d) son portefeuille de négociation est classé comme étant de faible taille au sens de l'article 94, paragraphe 1 du règlement CRR ;

e) la valeur totale de ses positions sur 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 %, ces deux pourcentages étant calculés conformément à l'article 273 bis, paragraphe 3 ;

f) plus de 75 % du total des actifs et des passifs consolidés de l'établissement, à l'exclusion, dans les deux cas, des expositions intragroupe, sont liés à des activités avec des contreparties situées dans l'Espace économique européen ;

g) l'établissement n'utilise pas de modèles internes pour satisfaire aux exigences prudentielles prévues par le présent règlement, 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 prévues à l'article 433 bis ou 433 quater du règlement CRR sur base consolidée ;

h) 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 ;

i) 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.

Cette définition d'établissement de petite taille et non complexe s'applique également aux sociétés de financement, les dispositions du règlement européen CRR s'appliquant également à cette catégorie d'entité en application de l'article 2 de l'arrêté du 23 novembre 2023 relatif au régime prudentiel des sociétés de financement.

Les sociétés de financement ne remplissant pas ces conditions et considérées comme les plus importantes en terme de taille devront appliquer les exigences découlant de la directive et du règlement DORA dès l'entrée en vigueur des dispositions pertinentes de ce projet de loi.

1.2. CADRE CONSTITUTIONNEL

Dans l'hypothèse où le juge constitutionnel examinerait la constitutionnalité de ces dispositions, le présent article n'est en contrariété avec aucune règle ou norme de valeur constitutionnelle.

La mesure relève du domaine de la loi en application de l'article 34 de la Constitution, au titre des obligations civiles et commerciales.

1.3. CADRE CONVENTIONNEL

Il n'y a pas de convention internationale sur le sujet.

1.4. ÉLEMENTS DE DROIT COMPARE

Les autres Etats membres de l'Union européenne modifieront également leur droit national d'ici le 17 janvier 2025 conformément à l'échéance établie par l'article 9 de la directive DORA.

2. NECESSITE DE LEGIFERER ET OBJECTIFS POURSUIVIS

2.1. NECESSITE DE LEGIFERER

La nécessité de légiférer provient ici de l'obligation constitutionnelle de transposition en droit interne d'une directive imposée par l'article 88-1 de la Constitution qui dispose que « [l]a République participe à l'Union européenne ». Cette obligation a d'ailleurs été rappelée par le Conseil constitutionnel dans le considérant 7 de sa décision n° 2004-496 DC du 10 juin 2004 : « Considérant qu'aux termes de l'article 88-1 de la Constitution […] ; qu'ainsi, la transposition en droit interne d'une directive communautaire résulte d'une exigence constitutionnelle à laquelle il ne pourrait être fait obstacle qu'en raison d'une disposition expresse contraire de la Constitution ».

2.2. OBJECTIFS POURSUIVIS

Cet article vise à octroyer aux entités les moins complexes et de taille plus petite un délai de mise en œuvre supplémentaire pour s'adapter aux exigences de la nouvelle directive DORA et du règlement associé.

L'introduction d'une proportionnalité des exigences et d'une progressivité dans le calendrier d'entrée en application est apparue pertinente dans la mesure où les sociétés de financement ne font pas partie des entités assujetties aux nouvelles exigences de résilience opérationnelle numérique listées à l'article 2(1) du règlement DORA. L'extension de ces exigences aux sociétés de financement dans le cadre de dispositions spécifiques en droit interne a été justifiée dans l'objectif de maintenir la comparabilité des exigences incombant aux établissements de crédit et aux sociétés de financement ainsi que dans l'objectif d'assurer la résilience opérationnelle numérique de l'ensemble du secteur financier français. Par ailleurs, La proportionnalité des exigences et la progressivité du calendrier d'entrée en application sont également apparues pertinentes dans la mesure où les dispositions de ce projet de loi étendent aux sociétés de financement le cadre le plus exigeant de gestion des risques informatiques prévu par le règlement DORA, à savoir les exigences du chapitre II du règlement (par rapport au cadre simplifié établi à l'article 16 du règlement qui aurait également pu constituer un régime applicable aux sociétés de financement en droit français).

Les sociétés de financement sont dans une grande proportion des entités de taille très modeste, si bien que peu d'entre elles franchissent le seuil en-deçà duquel sont définies les entités de petite taille et non complexes établi par l'article 4 du règlement CRR. Au sein des 144 sociétés de financement recensées, 135 d'entre elles répondent aux critères de qualification d'entité de petite taille et non complexe. De surcroît, celles-ci sont pour la plupart éloignées du seuil de cinq milliards d'euros du total des actifs puisque, au sein des 135 sociétés de financement dont le total des actifs est inférieur à cinq milliards d'euros, 124 d'entre elles disposent d'un total des actifs inférieur à deux milliards d'euros, et 117 d'entre elles disposent d'un total des actifs inférieur à un milliard d'euros.

Enfin, l'activité de la plupart des sociétés de financement apparaît par nature moins sensible pour l'économie que celle des établissements de crédit dans la mesure où les sociétés de financement ne sont pas autorisées à collecter des dépôts auprès du public.

3. OPTIONS POSSIBLES ET DISPOSITIF RETENU

3.1. OPTIONS ENVISAGEES

Suivant le principe du parallélisme des formes, une disposition législative ne peut être modifiée que par une mesure de même niveau normatif. Ainsi, aucune autre option que le recours à la loi n'a été envisagée ici.

3.2. OPTION RETENUE

Une entrée en application différée d'un an des articles 46, 47 et 54 du projet de loi ne pouvait qu'être inscrite dans ce même projet.

4. ANALYSE DES IMPACTS DES DISPOSITIONS ENVISAGEES

4.1. IMPACTS JURIDIQUES

4.1.1. Impacts sur l'ordre juridique interne

Entrée en application différée d'un an des modifications prévues aux articles L. 511-41-1-B, L. 511-55 et L. 612-24 du code monétaire et financier pour les sociétés de financement remplissant les conditions prévues au point 145 du paragraphe 1 de l'article 4 du règlement (UE) n° 575/2013 du Parlement européen et du Conseil dit « CRR ».

4.1.2. Articulation avec le droit international et le droit de l'Union européenne

L'article 9(1) de la directive DORA prévoit que les Etats membres adoptent les dispositions nécessaires pour se conformer et appliquent ces dispositions au plus tard le 17 janvier 2025. L'ensemble des dispositions visant à la mise en conformité de la France à l'égard de la directive DORA sont inclues au sein du titre III du projet de loi. Afin de d'assurer que la directive DORA soit transposée conformément au calendrier exigé par cette même directive, le présent article prévoit que les dispositions du titre III du projet de loi relatif à la résilience opérationnelle numérique entrent en application à compter du 17 janvier 2025.

Toutefois, le présent article introduit également une entrée en application différée – repoussée d'un an au 17 janvier 2026 – des articles 46, 47 et 54 de ce projet de loi pour les sociétés de financement remplissant les conditions prévues au point 145 du paragraphe 1 de l'article 4 du règlement (UE) n° 575/2013 du Parlement européen et du Conseil dit « CRR » qui définit les établissements de petite taille et non complexe.

4.2. IMPACTS ECONOMIQUES ET FINANCIERS

4.2.1. Impacts macroéconomiques

Sans objet.

4.2.2. Impacts sur les entreprises

Les sociétés de financement remplissant les conditions prévues au point 145 du paragraphe 1 de l'article 4 du règlement (UE) n° 575/2013 du Parlement européen et du Conseil dit « CRR » disposeront d'un délai supplémentaire d'un an par rapport à la date limite de transposition de la directive pour mettre leur dispositif de gouvernance et de gestion des risques liés aux TIC en conformité avec les exigences de la directive et du règlement DORA. Les sociétés de financement remplissant ces conditions sont a priori au nombre de 135. Seule une dizaine de sociétés de financement considérées notamment comme les plus importantes en termes de taille (dont la valeur totale des actifs serait supérieure cinq milliards d'euros) devront appliquer les exigences de la directive et du règlement européen au 17 janvier 2025.

4.2.3. Impacts budgétaires

4.3. IMPACTS SUR LES COLLECTIVITES TERRITORIALES

Sans objet.

4.4. IMPACTS SUR LES SERVICES ADMINISTRATIFS

L'entrée en application différée pour les sociétés de financement de petite taille et non complexe devrait se traduire par une charge moindre pour l'ACPR d'ici à janvier 2026.

4.5. IMPACTS SOCIAUX

4.5.1. Impacts sur la société

Sans objet.

4.5.2. Impacts sur les personnes en situation de handicap

Sans objet.

4.5.3. Impacts sur l'égalité entre les femmes et les hommes

Sans objet.

4.5.4. Impacts sur la jeunesse

Sans objet.

4.5.5. Impacts sur les professions réglementées

Sans objet.

4.6. IMPACTS SUR LES PARTICULIERS

Sans objet.

4.7. IMPACTS ENVIRONNEMENTAUX

Sans objet.

5. CONSULTATIONS ET MODALITES D'APPLICATION

5.1. CONSULTATIONS MENEES

En application de l'article L. 614-2 du code monétaire et financier, le Comité consultatif de la législation et de la réglementation financières (CCLRF) a été consulté a rendu un avis favorable le 23 mai 2024.

La rédaction proposée a en outre été soumise pour information et sur base informelle aux services du Secrétariat général de l'Autorité de contrôle prudentiel et de résolution (ACPR) et à l'Association française des Sociétés Financières (ASF).

5.2. MODALITES D'APPLICATION

5.2.1. Application dans le temps

Les dispositions du présent titre sont applicables à compter du 17 janvier 2025.

Toutefois, les dispositions des articles 46, 47 et 54 de la présente loi sont applicables aux sociétés de financement remplissant les conditions prévues au point 145 du paragraphe 1 de 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 aux entreprises d'investissement et modifiant le règlement (UE) n° 648/2012 à compter du 17 janvier 2026.

5.2.2. Application dans l'espace

Les dispositions du présent article relatives aux différentes entrées en vigueur différées s'appliquent à l'ensemble des territoires ultramarins.

5.2.3. Textes d'application

Le présent article ne requiert aucune disposition d'application.

PREMIER
MINISTRE
Liberté
Égalité
Fraternité

ANNEXE I – TABLEAU DE TRANSPOSITION DE LA DIRECTIVE (UE) 2022/2557 DU PARLEMENT EUROPEEN ET DU CONSEIL SUR LA RESILIENCE DES ENTITES CRITIQUES (DITE DIRECTIVE REC)

Disposition de la directive à transposer	Droit interne en vigueur modifié (code de la défense)	Nature juridique des normes à adopter pour assurer l'entière transposition de la directive	Dispositions proposées (code de la défense)	Observations générales et relatives à l'impact de la disposition de la directive
Article 1er 1. La présente directive : a) impose aux États membres l'obligation d'adopter des mesures spécifiques visant à garantir que les services qui sont essentiels au maintien de fonctions sociétales ou d'activités économiques vitales, dans le champ d'application de l'article 114 du traité sur le fonctionnement de l'Union européenne, soient fournis sans	Articles L. 1332-1 à L. 1332-7 (cf. détails *infra*)	Normes de nature législative dès lors que la directive impose aux Etats membres d'adopter des mesures relevant du domaine de la loi. L'ensemble de ces normes sera précisé par décret en Conseil d'Etat	Chapitre Ier du Titre Ier du projet de loi (cf. détails *infra*)	Ces dispositions ne sont pas transposées en tant que telles, car elles se bornent à fixer l'objet de la directive. En revanche, chacune des règles imposées aux *a), b) et c)* font l'objet de dispositions de transposition dans plusieurs articles du projet de loi (cf. détails *infra*)

entrave dans le marché intérieur, en particulier l'obligation de recenser les entités critiques et l'obligation d' aider les entités critiques à s'acquitter des obligations qui leur incombent ; b) impose aux entités critiques des obligations visant à renforcer leur résilience et leur capacité à fournir les services visés au point a) dans le marché intérieur ; c) établit des règles relatives : i) à la supervision des entités critiques ; ii) à l'exécution des règles ; iii) au recensement des entités critiques d'importance européenne particulière, ainsi qu'aux missions de conseil pour évaluer les mesures que ces entités ont mises en place pour				

satisfaire aux obligations qui leur incombent en vertu du chapitre III ; d) établit des procédures communes en matière de coopération et d'établissement de rapports sur l'application de la présente directive ; e) prévoit des mesures visant à atteindre un niveau élevé de résilience des entités critiques afin de garantir la fourniture de services essentiels dans l'Union et d'améliorer le fonctionnement du marché intérieur.				
2. La présente directive ne s'applique pas aux questions couvertes par la directive (UE) 2022/2555, sans préjudice de l'article 8 de la présente directive. La sécurité physique et la cybersécurité des entités critiques étant liées, les États	**Article L. 1332-6-1** Le Premier ministre fixe les règles de sécurité nécessaires à la protection des	Normes de nature législative s'agissant de mesures contraignantes imposées à des opérateurs et ayant un impact sur la liberté du commerce et de l'industrie ou sur la libre administration des	**Article L. 1332-11** I. – Pour gérer les risques qui menacent la sécurité des réseaux et des systèmes	Le Gouvernement s'est borné à fixer dans le titre Ier du projet de loi les obligations cyber qui s'imposent aux OIV, lesquelles sont exclusivement concernées par le titre II du projet de

membres veillent à ce que la présente directive et la directive (UE) 2022/2555 soient mises en œuvre de manière coordonnée.	systèmes d'information des opérateurs mentionnés aux articles L. 1332-1 et L. 1332-2 et des opérateurs publics ou privés qui participent à ces systèmes pour lesquels l'atteinte à la sécurité ou au fonctionnement risquerait de diminuer d'une façon importante le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la Nation ou pourrait présenter un danger grave pour la population. Ces opérateurs sont tenus d'appliquer ces règles à leurs frais. Les règles	collectivités territoriales L'ensemble de ces normes sera précisé par décret en Conseil d'Etat	d'information qu'ils utilisent dans le cadre de leurs activités ou de la fourniture de leurs services, les opérateurs d'importance vitale mettent en œuvre les obligations prévues aux articles 14 et 16 et au premier alinéa de l'article 17 de la loi n° XXX relative à la résilience des infrastructures critiques et au renforcement de la cybersécurité. II. – Pour répondre aux crises majeures menaçant ou affectant la sécurité des systèmes d'information, le Premier ministre peut décider des mesures que les	loi. Le choix a été fait de reprendre dans le titre Ier, au niveau législatif, celles des dispositions spécifiques à la sécurité des systèmes d'information figurant dans le code de la défense

	mentionnées au premier alinéa peuvent notamment prescrire que les opérateurs mettent en œuvre des systèmes qualifiés de détection des événements susceptibles d'affecter la sécurité de leurs systèmes d'information. Ces systèmes de détection sont exploités sur le territoire national par des prestataires de service qualifiés en matière de sécurité de systèmes d'information, par l'autorité nationale de sécurité des systèmes d'information ou par d'autres services de l'Etat désignés par le		opérateurs mentionnés au I de l'article L. 1332-2 doivent mettre en œuvre.	

	Premier ministre. Les qualifications des systèmes de détection et des prestataires de service exploitant ces systèmes sont délivrées par le Premier ministre. **Article L. 1332-6-2** Les opérateurs mentionnés aux articles L. 1332-1 et L. 1332-2 informent sans délai le Premier ministre des incidents affectant le fonctionnement ou la sécurité des systèmes d'information mentionnés au			

	premier alinéa de l'article L. 1332-6-1. **Article L. 1332-6-3** : A la demande du Premier ministre, les opérateurs mentionnés aux articles L. 1332-1 et L. 1332-2 soumettent leurs systèmes d'information à des contrôles destinés à vérifier le niveau de sécurité et le respect des règles de sécurité prévues à l'article L. 1332-6-1. Les contrôles sont effectués par l'autorité nationale de sécurité des systèmes			

	d'information ou par des services de l'Etat désignés par le Premier ministre ou par des prestataires de service qualifiés par ce dernier. Le coût des contrôles est à la charge de l'opérateur. **Article L. 1332-6-4** Pour répondre aux crises majeures menaçant ou affectant la sécurité des systèmes d'information, le Premier ministre peut décider des mesures que les opérateurs mentionnés aux articles L. 1332-1 et			

	L. 1332-2 doivent mettre en œuvre. **Article L. 1332-6-5** L'Etat préserve la confidentialité des informations qu'il recueille auprès des opérateurs mentionnés aux articles L. 1332-1 et L. 1332-2 dans le cadre de l'application de la présente section. **Article L. 1332-6-6** Un décret en Conseil d'Etat précise les conditions et limites			

	dans lesquelles s'appliquent les dispositions de la présente section			

3. Lorsque des dispositions d'actes juridiques sectoriels de l'Union exigent des entités critiques qu'elles adoptent des mesures pour renforcer leur résilience, et lorsque ces exigences sont reconnues par les États membres comme étant au moins équivalentes aux obligations correspondantes prévues par la présente directive, les dispositions pertinentes de la présente directive, y compris les dispositions relatives à la supervision et à l'exécution prévues au chapitre VI, ne s'appliquent pas. 4. Sans préjudice de l'article 346 du traité sur le fonctionnement de l'Union européenne, les informations qui sont confidentielles en application de règles de l'Union ou de règles nationales, telles que les règles relatives au secret des affaires,	Articles L. 1332-1 à L. 1332-7 (cf. détails *infra*)	Normes de nature législative dès lors que la directive impose aux Etats membres d'adopter des mesures relevant du domaine de la loi. L'ensemble de ces normes sera précisé par décret en Conseil d'Etat	Chapitre Ier du Titre Ier du projet de loi (cf. détails infra)	Ces dispositions ne sont pas transposées en tant que telles mais sont reprises en fonction des cas spécifiques qu'elles traitent. (cf. détails infra)

ne peuvent faire l'objet d'un échange avec la Commission et d'autres autorités concernées conformément à la présente directive que si cet échange est nécessaire à l'application de la présente directive. Les informations échangées se limitent à ce qui est nécessaire et proportionné à l'objectif de cet échange. L'échange d'informations préserve la confidentialité desdites informations ainsi que la sécurité et les intérêts commerciaux des entités critiques, tout en respectant la sécurité des États membres. 5. La présente directive est sans préjudice de la responsabilité des États membres en matière de sauvegarde de la sécurité nationale et de la défense et de leur pouvoir de garantir d'autres fonctions essentielles de l'État,				

notamment celles qui ont pour objet d'assurer l'intégrité territoriale de l'État et le maintien de l'ordre public. 6. La présente directive ne s'applique pas aux entités de l'administration publique qui exercent leurs activités dans les domaines de la sécurité nationale, de la sécurité publique, de la défense ou de l'application de la loi, y compris la détection des infractions pénales ainsi que les enquêtes et les poursuites en la matière 7. Les États membres peuvent décider que l'article 11 et les chapitres III, IV et VI, en tout ou en partie, ne s'appliquent pas à certaines entités critiques qui exercent des activités dans les domaines de la sécurité nationale, de la sécurité publique, de la défense ou de				

l'application de la loi, y compris la détection des infractions pénales ainsi que les enquêtes et les poursuites en la matière, ou qui fournissent des services exclusivement aux entités de l'administration publique visées au paragraphe 6 du présent article 8. Les obligations prévues dans la présente 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.				

9. La présente directive est sans préjudice du droit de l'Union relatif à la protection des données à caractère personnel, en particulier le règlement (UE) 2016/679 du Parlement européen et du Conseil et la directive 2002/58/CE du Parlement européen et du Conseil.	Sans objet	Sans objet	Sans objet	Sans objet
Article 2 Aux fins de la présente directive, on entend par : 1) « entité critique », une entité publique ou privée qui a été désignée par un État membre conformément à l'article 6 comme appartenant à l'une des catégories qui figurent dans la troisième colonne du tableau de l'annexe ;	**Article L. 1332-1** : Les opérateurs publics ou privés exploitant des établissements ou utilisant des installations et ouvrages, dont l'indisponibilité risquerait de diminuer d'une façon importante le potentiel de guerre ou économique, la sécurité ou la capacité	Normes de nature législative qui définissent le champ d'application des mesures qui seront imposées aux opérateurs concernés et qui ont nécessairement un impact sur la liberté du commerce et de l'industrie, sur la liberté d'entreprendre et sur la libre administration des collectivités territoriales. Ces normes seront	**Article L. 1332-2, I** Sont désignés opérateurs d'importance vitale par l'autorité administrative : 1° Les opérateurs publics ou privés exerçant, au moyen d'infrastructures critiques situées sur le territoire national, une activité d'importance vitale ;	Le Gouvernement ayant fait le choix de maintenir et d'adapter son dispositif actuel de sécurité des activités d'importance vitale en ayant recours à une rénovation de celui-ci plutôt qu'à une refonte, il a également fait le choix de conserver la notion d'opérateur d'importance vitale, bien connu des administrations, notamment locales, et des opérateurs. La notion d'entité critique,

	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. Ces établissements, installations ou ouvrages sont désignés par l'autorité administrative.	précisées par décret en Conseil d'Etat	L'autorité administrative précise, le cas échéant, dans l'acte de désignation de l'opérateur d'importance vitale, l'activité ou la liste des activités d'importance vitale exercées par l'opérateur qui constituent des services essentiels au fonctionnement du marché intérieur de l'Union européenne définis par le règlement délégué (UE) 2023/2450 de la Commission du 25 juillet 2023 complétant la directive (UE) 2022/2557 du Parlement européen et du Conseil en établissant une liste de services essentiels et qui, à ce titre, doivent être	au sens de la directive, correspond aux seuls OIV désignés au titre du I de l'article L. 1332-2 qui fournissent un service essentiel au fonctionnement du marché intérieur. Le second alinéa du 1° permet d'identifier ces entités critiques.

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

			l'environnement.	
2) « résilience », la capacité d'une entité critique à prévenir tout incident, à s'en protéger, à y réagir, à y résister, à l'atténuer, à l'absorber, à s'y adapter et à s'en rétablir ;	Sans objet		**Article L. 1332-3, 3e alinéa** Sur le fondement de cette analyse, les opérateurs d'importance vitale adoptent des mesures de résilience techniques, opérationnelles et organisationnelles, et proportionnées, afin d'assurer la continuité des activités d'importance vitale qu'ils exercent et de sauvegarder leurs infrastructures critiques	Le Gouvernement n'a pas souhaité reprendre au niveau législatif la définition de la résilience, celle-ci sera détaillée dans la partie réglementaire sur la définition du contenu des documents de planification.
3) « incident », un événement qui perturbe ou est susceptible	**L. 1332-6-2** : Les opérateurs	Norme de nature législative dès lors qu'elle	**Article L. 1332-7** : Les opérateurs	Sans être mentionnée explicitement, la notion

de perturber de manière importante la fourniture d'un service essentiel, y compris lorsqu'il affecte les systèmes nationaux qui préservent l'état de droit ;	mentionnés aux articles L. 1332-1 et L. 1332-2 informent sans délai le Premier ministre des incidents affectant le fonctionnement ou la sécurité des systèmes d'information mentionnés au premier alinéa de l'article L. 1332-6-1.	vise le champ d'application des dispositions imposant la notification des incidents	d'importance vitale désignés au titre du 1° du I de l'article L. 1332-2 notifient à l'autorité administrative tout incident susceptible de compromettre la continuité de ses activités d'importance vitale dans un délai prévu par décret en Conseil d'Etat. L'autorité administrative informe le public de cet incident lorsqu'elle estime qu'il est dans l'intérêt général de le faire.	d'incident telle que reprise à cet article transpose la directive en faisant référence aux incidents ayant un impact sur la continuité des activités d'importance vitale, notion plus large que celle de service essentiel et qui la contient.
4) « infrastructure critique », un bien, une installation, un équipement, un réseau ou un système, ou une partie d'un bien, d'une installation, d'un	**L. 1332-1** : Les opérateurs publics ou privés exploitant des établissements ou utilisant des	Normes de nature législative qui définissent le champ d'application des mesures qui seront imposées aux opérateurs	**Article L. 1332-1, 2° :** Infrastructure critique : tout ou partie d'un bien, d'une installation, d'un équipement, d'un réseau	Dans une logique commune pour l'ensemble de la transposition, le Gouvernement ayant privilégié le maintien d'un

équipement, d'un réseau ou d'un système, qui est nécessaire à la fourniture d'un service essentiel ;	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. Ces établissements, installations ou ouvrages sont désignés par l'autorité administrative.	concernés et qui ont nécessairement un impact sur la liberté du commerce et de l'industrie, sur la liberté d'entreprendre et sur la libre administration des collectivités territoriales. Ces normes seront précisées par décret en Conseil d'Etat	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 ; Parmi les infrastructures critiques, on distingue notamment : - Les points d'importance vitale, c'est-à-dire les installations les plus sensibles, notamment celles qui sont difficilement substituables ;	dispositif bien établi et connu, le choix a été fait de mentionner directement dans la loi celles des définitions issues de la directive tout en les simplifiant et en permettant une exacte corrélation avec des notions connues. Pour ce qui concerne les infrastructures critiques, cette catégorie est plus englobante que celles déjà en vigueur de points d'importance vitale (PIV) et de systèmes d'information d'importance vitale, notions conservées. La notion d'infrastructure critique est employée dans l'un des critères de recensement des entités critiques de la directive, elle est donc également employée pour la désignation des OIV (voir

			- Les systèmes d'information d'importance vitale, c'est-à-dire les systèmes d'information nécessaires à l'exercice d'une activité d'importance vitale ou à la gestion, l'utilisation ou la protection d'une ou plusieurs infrastructures critiques	L1332-2), notion englobant les entités critiques. Le fait de ne pas assimiler la notion d'infrastructure critique à celle de PIV permettra par ailleurs de pouvoir désigner des OIV sans PIV, ce qui offrira plus de souplesse au dispositif. La notion de nécessité à la fourniture d'un service essentiel de la directive correspond à la formulation proposée, à savoir celle d'une infrastructure 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 lorsque l'opérateur est désigné au

				titre du 2° de l'article L. 1332-1 (« SEVESO »)
5) « service essentiel », un service qui est crucial pour le maintien de fonctions sociétales ou d'activités économiques vitales, de la santé publique et de la sûreté publique, ou de l'environnement ;	Sans objet (dans la partie législative)		**Article L. 1332-1, 1° :** Activités d'importance vitale : les activités indispensables au fonctionnement de l'économie, de la société, à la défense ou à la sécurité de la Nation.	Dans la même logique que celle développée s'agissant de la définition des infrastructures critiques, la notion d'activités d'importance vitale étant celle connue des opérateurs, son emploi a été conservé. Les services essentiels définis par la directive sont donc des activités d'importance vitale exercées dans l'un des secteurs visés par la directive et listés dans l'acte délégué dédié. Ce choix résulte de la volonté du Gouvernement de ne pas dégrader son

				système actuel en ayant pris soin de conserver celles des activités d'importance vitale qui ne sont pas des services essentiels et/ou qui ne rentrent pas dans le champ d'application de la directive, et donc de continuer à appliquer le dispositif à ces opérateurs particulièrement sensibles (activités militaires de l'Etat notamment).
6) « risque », le potentiel de perte ou de perturbation causé par un incident, à exprimer comme la combinaison de l'ampleur de cette perte ou de cette perturbation et la probabilité que l'incident se produise ;	Sans objet	Normes de nature législative dès lors qu'elles font référence au contenu des obligations imposées aux opérateurs qui doivent réaliser une analyse de risque. L'ensemble de ces normes	**Article L. 1332-3, alinéa 1 à 4** : Les opérateurs d'importance vitale réalisent une analyse des risques de toute nature, y compris à caractère terroriste, qui pourraient	Le Gouvernement a fait le choix de reprendre les notions de la directive dans le cadre des mesures imposées aux opérateurs. Ces mesures peuvent être regardées comme transposant ces définitions

7) « évaluation des risques », l'ensemble du processus permettant de déterminer la nature et l'étendue d'un risque en déterminant et en analysant les menaces, les vulnérabilités et les dangers potentiels pertinents qui pourraient conduire à un incident et en évaluant la perte ou la perturbation potentielle de la fourniture d'un service essentiel causée par cet incident ;		sera précisé par décret en Conseil d'Etat	perturber l'exercice de leurs activités d'importance vitale ou la sécurité de leurs infrastructures critiques, notamment des points d'importance vitale désignés par l'autorité administrative. Cette analyse est réalisée au plus tard dans un délai de neuf mois à compter de la désignation prévue au I de l'article L. 1332-2 et réévaluée au moins tous les quatre ans. Sur le fondement de cette analyse, les opérateurs d'importance vitale adoptent des mesures de résilience techniques,	en les reprenant.

			opérationnelles et organisationnelles, et proportionnées, afin d'assurer la continuité des activités d'importance vitale qu'ils exercent et de sauvegarder leurs infrastructures critiques. L'analyse des risques ainsi que les mesures de résilience sont détaillées dans un document dénommé "plan de résilience opérateur" élaboré par l'opérateur, au plus tard dans un délai de dix mois à compter de la désignation prévue au I de l'article L. 1332-2, et approuvé par l'autorité administrative.	

8) « norme », une norme au sens de l'article 2, point 1), du règlement (UE) no 1025/2012 du Parlement européen et du Conseil (30); 9) « spécification technique », une spécification technique au sens de l'article 2, point 4), du règlement (UE) no 1025/2012 ; 10) « entité de l'administration publique », une entité reconnue comme telle dans un État membre conformément au droit national, à l'exclusion de l'organisation judiciaire, des parlements et des banques centrales, qui satisfait aux critères suivants : a) elle a été créée pour satisfaire des besoins d'intérêt général et n'a pas de caractère industriel ou commercial ; b) elle est dotée de la	Sans objet	Sans objet	Sans objet	Aucune de ces définitions ne nécessite d'être transposée pour être rendue opérationnelles

personnalité juridique ou est juridiquement habilitée à agir pour le compte d'une autre entité dotée de la personnalité juridique ; c) elle est financée majoritairement par les autorités de l'État ou d'autres organismes de droit public de niveau central, ou sa gestion est soumise à un contrôle de la part de ces autorités ou organismes, ou son organe d'administration, de direction ou de surveillance est composé, pour plus de la moitié, de membres désignés par les autorités de l'État ou d'autres organismes de droit public de niveau central ; d) elle a le pouvoir d'adresser à des personnes physiques ou morales des décisions administratives ou réglementaires affectant leurs				

droits en matière de mouvements transfrontières des personnes, des biens, des services ou des capitaux.				
Article 3 : La présente directive ne fait pas obstacle à l'adoption ou au maintien par les États membres de dispositions de droit national afin d'atteindre un niveau plus élevé de résilience des entités critiques, à condition que ces dispositions soient compatibles avec les obligations des États membres prévues par le droit de l'Union.	Sans objet	Sans objet	Sans objet	Sans objet
Article 4 **Stratégie pour la résilience des entités critiques** 1. À la suite d'une consultation qui est, dans la mesure du	Sans objet	Sans objet	Sans objet	Ces deux dispositions concernant les Etats membres ne nécessitent pas de mesure de transposition mais seront appliquées dans le cadre de la stratégie

possible en pratique, ouverte aux parties prenantes concernées, chaque État membre adopte, au plus tard le 17 janvier 2026, une stratégie visant à renforcer la résilience des entités critiques (ci-après dénommée « stratégie »). La stratégie définit des objectifs stratégiques et des mesures politiques, en s'appuyant sur des stratégies nationales et sectorielles, des plans ou des documents similaires pertinents existants, en vue d'atteindre et de maintenir un niveau élevé de résilience des entités critiques et de couvrir au moins les secteurs figurant à l'annexe. 2. Chaque stratégie contient au moins les éléments suivants : a) les objectifs stratégiques et les priorités aux fins de renforcer la résilience globale des entités				nationale de résilience.

critiques, compte tenu des dépendances et des interdépendances transfrontières et transsectorielles ; b) un cadre de gouvernance permettant d'atteindre les objectifs stratégiques et les priorités, y compris une description des rôles et des responsabilités des différentes autorités, entités critiques et autres parties participant à la mise en œuvre de la stratégie ; c) une description des mesures nécessaires pour renforcer la résilience globale des entités critiques, y compris une description de l'évaluation des risques visée à l'article 5 ; d) une description du processus par lequel les entités critiques sont recensées ; e) une description du processus				

de soutien aux entités critiques conformément au présent chapitre, y compris les mesures visant à renforcer la coopération entre le secteur public, d'une part, et le secteur privé et les entités publiques et privées, d'autre part ; f) une liste des principales autorités et parties prenantes concernées, autres que les entités critiques, participant à la mise en œuvre de la stratégie ; g) un cadre d'action pour la coordination entre les autorités compétentes en vertu de la présente directive (ci-après dénommées « autorités compétentes ») et les autorités compétentes en vertu de la directive (UE) 2022/2555 aux fins du partage d'informations sur les risques, menaces et incidents en matière de				

cybersécurité ainsi que sur les risques, menaces et incidents non liés à la cybersécurité, et de l'exercice des tâches de supervision ; h) une description des mesures déjà en place visant à faciliter la mise en œuvre des obligations prévues au chapitre III de la présente directive par les petites et moyennes entreprises au sens de l'annexe de la recommandation 2003/361/CE de la Commission (31) que les États membres concernés ont recensées en tant qu'entités critiques. À la suite d'une consultation qui est, dans la mesure du possible en pratique, ouverte aux parties prenantes concernées, les États membres mettent à jour leur stratégie au moins tous les quatre ans.				

3. Les États membres communiquent leur stratégie et leurs mises à jour substantielles à la Commission dans un délai de trois mois à compter de leur adoption. **Article 5** **Évaluation des risques par les États membres** 1. La Commission est habilitée à adopter un acte délégué, conformément à l'article 23, au plus tard le 17 novembre 2023, afin de compléter la présente directive en établissant une liste non exhaustive de services essentiels dans les secteurs et les sous-secteurs figurant à l'annexe. Les autorités compétentes utilisent ladite liste des services essentiels pour effectuer une évaluation des risques (ci-après dénommée « évaluation des risques d'État				

membre ») au plus tard le 17 janvier 2026, puis selon les besoins, et au moins tous les quatre ans. Les autorités compétentes utilisent les évaluations des risques d'États membres aux fins de recenser les entités critiques conformément à l'article 6 et pour aider les entités critiques à adopter des mesures en vertu de l'article 13. Les évaluations des risques d'États membres rendent compte des risques naturels et d'origine humaine pertinents, y compris ceux qui revêtent un caractère transsectoriel ou transfrontière, des accidents, des catastrophes naturelles, des urgences de santé publique et des menaces hybrides ou autres menaces antagonistes, lesquelles comprennent les infractions terroristes prévues par la directive (UE) 2017/541 du				

Parlement européen et du Conseil (32). 2. Lorsqu'ils procèdent à des évaluations des risques d'États membres, les États membres tiennent compte au moins des éléments suivants : a) l'évaluation des risques générale effectuée en vertu de l'article 6, paragraphe 1, de la décision n° 1313/2013/UE ; b) d'autres évaluations des risques pertinentes effectuées conformément aux exigences des actes juridiques sectoriels pertinents de l'Union, y compris les règlements (UE) 2017/1938 (33) et (UE) 2019/941 (34) du Parlement européen et du Conseil, ainsi que les directives 2007/60/CE (35) et 2012/18/UE (36) du Parlement européen et du Conseil ;				

c) les risques pertinents découlant de la mesure dans laquelle les secteurs figurant à l'annexe dépendent les uns des autres, y compris de la mesure dans laquelle ils dépendent d'entités situées dans d'autres États membres et des pays tiers, et l'incidence qu'une perturbation importante dans un secteur peut avoir sur d'autres secteurs, y compris tout risque importante pour les citoyens et le marché intérieur ; d) toute information sur les incidents notifiés conformément à l'article 15. Aux fins du premier alinéa, point c), les États membres coopèrent avec les autorités compétentes d'autres États membres et les autorités compétentes de pays tiers, s'il y a lieu. 3. Les États membres mettent à				

la disposition des entités critiques qu'ils ont recensées conformément à l'article 6, s'il y a lieu par l'intermédiaire de leur point de contact unique, les éléments pertinents des évaluations des risques d'États membres. Les États membres veillent à ce que les informations fournies aux entités critiques aident ces dernières à réaliser leurs évaluations des risques en vertu de l'article 12, et à adopter des mesures pour garantir leur résilience en vertu de l'article 13. 4. Dans un délai de trois mois à compter de la réalisation d'une évaluation des risques d'État membre, l'État membre fournit à la Commission des informations pertinentes sur les types de risques recensés suivant cette évaluation des risques d'État membre et les résultats de				

l'évaluation des risques d'État membre, par secteur et sous-secteur figurant à l'annexe. 5. La Commission, en coopération avec les États membres, élabore un modèle commun facultatif de rapport aux fins du respect du paragraphe 4.				
Article 6 **Recensement des entités critiques** 1. Au plus tard le 17 juillet 2026, chaque État membre recense les entités critiques pour les secteurs et sous-secteurs figurant à l'annexe. 2. Lorsqu'un État membre recense les entités critiques en vertu du paragraphe 1, il tient	**L. 1332-1** : Les opérateurs publics ou privés exploitant des établissements ou utilisant des installations et ouvrages, dont l'indisponibilité risquerait de diminuer d'une façon importante le potentiel de guerre ou économique, la	Normes de niveau législatif pour la désignation des opérateurs d'importance vitale, qui sont également désignés entités critiques au sens de la directive lorsqu'ils fournissent un service essentiel et qui seront soumis aux obligations de résilience Un décret en Conseil d'Etat précisera	**Article L. 1332-1, I et II :** I. - Sont désignés opérateurs d'importance vitale par l'autorité administrative : 1° Les opérateurs publics ou privés exerçant, au moyen d'infrastructures critiques situées sur le	L'Etat français a, depuis l'origine, fait le choix de désigner les opérateurs d'importance vitale afin de les recenser. Ce choix est maintenu dans le cadre de la transposition de cet article. La désignation en tant qu'entité critique repose sur les trois critères mentionnés

compte des résultats de son évaluation des risques d'État membre et de sa stratégie et applique tous les critères suivants : a) l'entité fournit un ou plusieurs services essentiels ; b) l'entité exerce ses activités sur le territoire dudit État membre et son infrastructure critique est située sur ledit territoire ; et c) un incident aurait des effets perturbateurs importants, déterminés conformément à l'article 7, paragraphe 1, sur la fourniture par l'entité d'un ou de plusieurs services essentiels ou sur la fourniture d'autres services essentiels dans les secteurs figurant à l'annexe qui dépendent dudit ou desdits services essentiels.	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. Ces établissements, installations ou ouvrages sont désignés par l'autorité administrative. **Article L. 1332-2 :** Les obligations prescrites par le présent chapitre	l'ensemble du dispositif	territoire national, une activité d'importance vitale ; L'autorité administrative précise, le cas échéant, dans l'acte de désignation de l'opérateur d'importance vitale, l'activité ou la liste des activités d'importance vitale exercées par l'opérateur qui constituent des services essentiels au fonctionnement du marché intérieur de l'Union européenne définis par le règlement délégué (UE) 2023/2450 de la Commission du 25 juillet 2023 complétant la directive (UE) 2022/2557 du Parlement européen et	par la directive : - Fourniture d'un « service essentiel » ; ici, c'est la notion d'activité d'importance vitale qui a été privilégiée, pour inclure les services essentiels et les autres activités sensibles non couvertes par la directive ; l'autorité administrative précisera le cas échéant la liste des services essentiels fournis ; - Exercice d'une activité sur le territoire au moyen d'infrastructures critiques ; - Incident ayant des « effets perturbateurs

3. Chaque État membre dresse une liste des entités critiques recensées en vertu du paragraphe 2 et veille à ce que ces entités critiques reçoivent notification de ce qu'elles ont été recensées en tant qu'entités critiques dans un délai d'un mois à compter de ce recensement. Les États membres informent ces entités critiques des obligations qui leur incombent en vertu des chapitres III et IV et de la date à partir de laquelle ces obligations leur sont applicables, sans préjudice de l'article 8. Les États membres informent les entités critiques des secteurs figurant aux points 3, 4 et 8 du tableau de l'annexe qu'elles ne sont soumises à aucune des obligations prévues aux chapitres III et IV, sauf mesures nationales contraires.	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. Ces établissements sont désignés par l'autorité administrative.		du Conseil en établissant une liste de services essentiels et qui, à ce titre, doivent être regardés comme des entités critiques au sens de cette directive ; 2° Les opérateurs publics ou privés, gestionnaires, propriétaires ou exploitants d'établissements mentionnés à l'article L. 511-1 du code de l'environnement ou comprenant une installation nucléaire de base mentionnée à l'article L. 593-2 du même code, lorsque la destruction ou l'avarie d'une ou plusieurs installations de ces	importants » ; cette notion n'est pas formellement reprise dans la loi ; le système actuel sera conservé, à savoir que les directives nationales de sécurité prises par chaque ministère coordonnateur fixera les critères d'identification précis des opérateurs dans chaque secteur, notamment des seuils, en suivant les types de paramètres listés par la directive. Ces critères sont repris dans la rédaction proposée de l'article L. 1332-2 tout en

			établissements peut présenter un danger d'une particulière gravité pour la population ou l'environnement. II. – Ces opérateurs mettent en œuvre, à leurs frais, les obligations leur incombant prévues au présent chapitre.	maintenant le socle commun. Ainsi, tous les opérateurs d'importance vitale ne seront pas nécessairement considérés comme entités critiques au sens de la directive et donc ces opérateurs ne seront pas soumis à la seule exigence supplémentaire applicable lorsqu'ils fournissent un service essentiel et que ce service essentiel est fourni dans au moins 6 Etats membres (secteurs régaliens exclus de la directive).
Le chapitre III s'applique aux entités critiques concernées dix mois suivant la date de la notification visée au premier	Sans objet	Norme de nature législative qui précise le délai accordé aux opérateurs, lors de leur	**Article L. 1332-3, alinéas 1 à 4** Les opérateurs	Le maintien du dispositif actuel de sécurité des activités importances vitales a conduit le Gouvernement

alinéa du présent paragraphe.		désignation, pour se conformer aux exigences du chapitre III de la directive sur les mesures de résilience à adopter : - Evaluation des risques ; - Adoption de mesures techniques, de sécurité et organisationnelles appropriées et proportionnées pour garantir leur résilience ; - Vérification des antécédents ; - Notification des incidents.	d'importance vitale réalisent une analyse des risques de toute nature, y compris à caractère terroriste, qui pourraient perturber l'exercice de leurs activités d'importance vitale ou la sécurité de leurs infrastructures critiques, notamment des points d'importance vitale désignés par l'autorité administrative. Cette analyse est réalisée au plus tard dans un délai de neuf mois à compter de la désignation prévue au I de l'article L. 1332-2 et réévaluée au moins tous les quatre ans.	à conserver une logique de planification et a donc opté pour une évolution des documents de planification existants. Les mesures de résilience seront donc, après réalisation de l'analyse des risques, détaillées dans le plan de résilience opérateur

			Sur le fondement de cette analyse, les opérateurs d'importance vitale adoptent des mesures de résilience techniques, opérationnelles et organisationnelles, et proportionnées, afin d'assurer la continuité des activités d'importance vitale qu'ils exercent et de sauvegarder leurs infrastructures critiques. L'analyse des risques ainsi que les mesures de résilience sont détaillées dans un document dénommé "plan de résilience opérateur" élaboré par l'opérateur, au plus tard dans un délai de dix mois à compter de	

			la désignation prévue au I de l'article L. 1332-2, et approuvé par l'autorité administrative.	
4. Les États membres veillent à ce que leurs autorités compétentes en vertu de la présente directive notifient aux autorités compétentes en vertu de la directive (UE) 2022/2555 l'identité des entités critiques qu'ils ont recensées en vertu du présent article dans un délai d'un mois à compter dudit recensement. Cette notification précise, le cas échéant, que les entités critiques concernées sont des entités des secteurs figurant aux points 3, 4 et 8 du tableau de l'annexe de la présente directive et qu'elles ne sont soumises à aucune des obligations prévues aux chapitres III et IV de la présente directive.	Sans objet	Sans objet	Sans objet	Ces dispositions concernant les Etats membres ne nécessitent pas de mesures de transposition mais seront bien mises en œuvre par le Gouvernement. Ces points pourraient être rappelés dans le cadre de la révision des textes réglementaires d'application, notamment

5. Si nécessaire et en tout état de cause au moins tous les quatre ans, les États membres réexaminent et, s'il y a lieu, mettent à jour la liste des entités critiques recensées visées au paragraphe 3. Lorsque ces mises à jour entraînent le recensement d'entités critiques supplémentaires, les paragraphes 3 et 4 s'appliquent à ces entités critiques supplémentaires. En outre, les États membres veillent à ce que les entités qui ne sont plus recensées en tant qu'entités critiques à la suite d'une telle mise à jour reçoivent notification en temps utile de ce fait et du fait qu'elles ne sont plus soumises aux obligations prévues au chapitre III à compter de la date de réception de cette notification. 6. La Commission élabore, en coopération avec les États				

membres, des recommandations et des lignes directrices non contraignantes pour soutenir les États membres dans leur recensement des entités critiques.				
Article 7 **Effet perturbateur important** 1. Lorsqu'ils déterminent l'importance d'un effet perturbateur visé à l'article 6, paragraphe 2, point c), les États membres prennent en compte les critères suivants : a) le nombre d'utilisateurs tributaires du service essentiel fourni par l'entité concernée ; b) la mesure dans laquelle les autres secteurs et sous-secteurs figurant à l'annexe dépendent du service essentiel en question ;	**L. 1332-1 :** Les opérateurs publics ou privés exploitant des établissements ou utilisant des installations et ouvrages, dont l'indisponibilité risquerait de diminuer d'une façon importante le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la nation, sont tenus de coopérer à leurs frais dans les conditions définies au	Normes de nature législative qui définissent le champ d'application des mesures qui seront imposées aux opérateurs concernés et qui ont nécessairement un impact sur la liberté du commerce et de l'industrie, sur la liberté d'entreprendre et sur la libre administration des collectivités territoriales. Ces normes seront précisées par décret en Conseil d'Etat	**Article L. 1332-1, 1° :** Activités d'importance vitale : les activités indispensables au fonctionnement de l'économie, de la société, à la défense ou à la sécurité de la Nation. **Article L. 1332-2, I :** Sont désignés opérateurs d'importance vitale par l'autorité administrative :	S'agissant d'éléments d'appréciation tenant à la désignation des opérateurs soumis aux obligations de résilience, le Gouvernement a privilégié de ne pas alourdir inutilement le projet de loi en adoptant une disposition spécifique pour transposer cet article. En effet, pour ce faire, il a été préféré de s'en remettre à des notions, qui englobent celles de la directive, précédemment étayées, à savoir : - la réalisation d'une activité

c) l'impact que des incidents pourraient avoir, du point de vue de l'ampleur et de la durée, sur les activités économiques et sociétales, l'environnement, la sûreté et la sécurité publiques, ou la santé de la population ; d) la part de marché de l'entité sur le marché du ou des services essentiels concernés ; e) la zone géographique susceptible d'être affectée par un incident, y compris toute incidence transfrontière, compte tenu de la vulnérabilité associée au degré d'isolement de certains types de zones géographiques, telles que les régions insulaires, les régions éloignées ou les zones montagneuses ; f) l'importance que revêt l'entité pour le maintien d'un niveau suffisant de service essentiel, compte tenu de la disponibilité	présent chapitre, à la protection desdits établissements, installations et ouvrages contre toute menace, notamment à caractère terroriste. Ces établissements, installations ou ouvrages sont désignés par l'autorité administrative. **L. 1332-2 :** Les obligations prescrites par le présent chapitre peuvent être étendues à des établissements mentionnés à l'article L. 511-1 du code de l'environnement ou comprenant une installation nucléaire		1° Les opérateurs publics ou privés exerçant, au moyen d'infrastructures critiques situées sur le territoire national, une activité d'importance vitale ; L'autorité administrative précise, le cas échéant, dans l'acte de désignation de l'opérateur d'importance vitale, l'activité ou la liste des activités d'importance vitale exercées par l'opérateur qui constituent des services essentiels au fonctionnement du marché intérieur de l'Union européenne définis par le règlement délégué (UE) 2023/2450	d'importance vitale c'est-à-dire indispensable au fonctionnement de l'économie, de la société, à la défense ou à la sécurité de la nation ; une telle activité peut être un service essentiel au sens de la directive ; - au moyen d'une ou plusieurs infrastructures critiques 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. L'appréciation portant sur ces deux critères repose donc, pour les opérateurs relevant du champ d'application de la directive, sur une analyse de

de solutions de rechange pour la fourniture de ce service essentiel.	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. Ces établissements sont désignés par l'autorité administrative.		de la Commission du 25 juillet 2023 complétant la directive (UE) 2022/2557 du Parlement européen et du Conseil en établissant une liste de services essentiels et qui, à ce titre, doivent être regardés comme des entités critiques au sens de cette directive ; 2° Les opérateurs publics ou privés, gestionnaires, propriétaires ou exploitants d'établissements mentionnés à l'article L. 511-1 du code de l'environnement ou comprenant une installation nucléaire de base mentionnée à l'article L. 593-2 du	l'importance de l'effet perturbateur qui conduira le cas échéant à la désignation comme opérateur d'importance vital et donc d'entité critique au sens de la directive. Celle si reposera sur les éléments fixés dans chaque directive nationale de sécurité, pour chaque secteur et sous-secteur (voir supra).

			même code, lorsque la destruction ou l'avarie d'une ou plusieurs installations de ces établissements peut présenter un danger d'une particulière gravité pour la population ou l'environnement.	
2. Après le recensement des entités critiques en vertu de l'article 6, paragraphe 1, chaque État membre communique les informations suivantes à la Commission, sans retard injustifié : a) une liste de services essentiels dans ledit État membre lorsqu'il existe des services essentiels supplémentaires par rapport à la liste des services essentiels visée à l'article 5, paragraphe 1 ;	Sans objet	Sans objet	Sans objet	Cette disposition concernant les Etats membres ne nécessite pas de mesure de transposition mais sera bien mise en œuvre par le Gouvernement

b) le nombre d'entités critiques recensées pour chaque secteur et sous-secteur figurant à l'annexe et pour chaque service essentiel ; c) les seuils éventuellement appliqués en vue de préciser un ou plusieurs des critères du paragraphe 1. Les seuils visés au premier alinéa, point c), peuvent être présentés tels quels ou sous une forme agrégée. Les États membres communiquent ensuite les informations visées au premier alinéa, chaque fois que cela est nécessaire et au moins tous les quatre ans. 3. Après consultation du groupe sur la résilience des entités critiques visé à l'article 19, la Commission adopte des lignes directrices non				

contraignantes pour faciliter l'application des critères visés au paragraphe 1 du présent article, en tenant compte des informations visées au paragraphe 2 du présent article.				
Article 8 : **Entités critiques des secteurs des banques, des infrastructures des marchés financiers et des infrastructures numériques** Les États membres veillent à ce que l'article 11 et les chapitres III, IV et VI ne s'appliquent pas aux entités critiques qu'ils ont recensées dans les secteurs figurant aux points 3, 4 et 8 du tableau de l'annexe. Les États membres peuvent adopter ou maintenir des dispositions de droit national afin d'atteindre un niveau de résilience plus élevé	Sans objet	Sans objet	Sans objet	Cette disposition ne nécessite pas de mesure particulière, ces secteurs étant couverts par la directive et le règlement « DORA » (cf. titre III du projet de loi) et par la directive NIS2, également transposée.

pour ces entités critiques à condition que ces dispositions soient compatibles avec le droit de l'Union applicable.				
Article 9 : **Autorités compétentes et point de contact unique** 1. Chaque État membre désigne ou met en place une ou plusieurs autorités compétentes chargées de veiller à l'application correcte des règles énoncées dans la présente directive au niveau national et, si nécessaire, de les faire respecter. En ce qui concerne les entités critiques des secteurs figurant aux points 3 et 4 du tableau de l'annexe de la présente directive, les autorités compétentes sont, en principe, les autorités	**Article L. 1332-3** : Les opérateurs dont un ou plusieurs établissements, installations et ouvrages sont désignés en application du présent chapitre réalisent pour chacun d'eux les mesures de protection prévues à un plan particulier de protection dressé par l'opérateur et approuvé par l'autorité administrative. Ces mesures	Normes de nature législative pour préciser les modalités de désignation des agents chargés du contrôle ainsi que pour préciser l'étendue de leurs pouvoirs et les garanties accordées à l'opérateur contrôlé. Ces mesures seront précisées par décret en Conseil d'Etat	**Article L. 1332-12** : Sont habilités à rechercher et constater les infractions et manquements aux prescriptions du présent chapitre, à l'exception de l'article L. 1332-11, ainsi qu'aux dispositions réglementaires prises pour son application, en vue de la saisine de la commission prévue à l'article L. 1332-15, les agents de l'Etat spécialement désignés et assermentés à cette fin dans des conditions	Ces dispositions du projet de loi transposent le 1 de l'article 9 selon les choix retenus par le Gouvernement à savoir : - De ne pas créer un corps d'inspection dédié mais de permettre à chaque ministre coordonnateur (cf. introduction de l'étude d'impact) de désigner ceux des agents dont les qualifications et compétences répondent aux exigences de la directive ; il en est de même pour les agents chargés du suivi du dispositif au niveau local,

compétentes visées à l'article 46 du règlement (UE) 2022/2554 En ce qui concerne les entités critiques du secteur figurant au point 8 du tableau de l'annexe de la présente directive, les autorités compétentes sont, en principe, les autorités compétentes en vertu de la directive (UE) 2022/2555. Les États membres peuvent désigner une autorité compétente différente pour les secteurs figurant aux points 3, 4 et 8 du tableau de l'annexe de la présente directive conformément aux cadres nationaux existants. Lorsqu'ils désignent ou mettent en place plus d'une autorité compétente, les États membres définissent clairement les tâches de chacune des autorités concernées et veillent à ce qu'elles coopèrent efficacement pour accomplir les tâches qui	comportent notamment des dispositions efficaces de surveillance, d'alarme et de protection matérielle. En cas de non-approbation du plan et de désaccord persistant, la décision est prise par l'autorité administrative. **L. 1332-4 :** En cas de refus des opérateurs de préparer leur plan particulier de protection, l'autorité administrative met, par arrêtés, les chefs d'établissements ou d'entreprises assujettis en demeure de l'établir dans le délai qu'elle fixe.		précisées par décret en Conseil d'Etat. **Article L. 1332-13 :** Les agents mentionnés à l'article L. 1332-12 ont accès, pour l'exercice de leurs missions, aux locaux des opérateurs d'importance vitale. Ils peuvent pénétrer dans les lieux à usage professionnel ou dans les lieux d'exécution d'une prestation de service. Ils peuvent accéder à tout document nécessaire à l'accomplissement de leur mission auprès des administrations publiques, des	dans les préfectures de départements et les états-majors de zone de défense; - De donner à ces agents des garanties dans la conduite de leur mission tout en encadrant leur mise en œuvre ; - De prévenir les risques liés au déroulement du contrôle en sanctionnant les entraves ; - De sécuriser juridiquement les constatations lesquelles peuvent être à l'origine de sanctions administratives. Le dispositif actuellement en vigueur ne prévoit que le cas de mise en demeure de réaliser le plan particulier de protection qui relève de la

leur incombent en vertu de la présente directive, y compris en ce qui concerne la désignation et les activités du point de contact unique visé au paragraphe 2.	**L. 1332-5 :** Le plan de protection établi dans les conditions prévues à l'article L. 1332-4, l'autorité administrative met, par arrêtés, les chefs d'établissements ou d'entreprises en demeure de le réaliser dans le délai qu'elle fixe. **L. 1332-6 :** Les arrêtés de mise en demeure prévus aux articles L. 1332-4 et L. 1332-5 fixent un délai qui ne peut être inférieur à un mois, et qui est déterminé en tenant compte des conditions de fonctionnement de		établissements et organismes placés sous le contrôle de l'Etat et des collectivités territoriales, ainsi que dans les entreprises ou services concédés par l'Etat, les régions, les départements et les communes. Ils peuvent recueillir, sur place ou sur convocation, tout renseignement, toute justification ou tout document nécessaire aux contrôles. A ce titre, ils peuvent exiger la communication de documents de toute nature propres à faciliter l'accomplissement de leur mission. Ils peuvent les obtenir ou en prendre copie, par tout moyen et	compétence de l'autorité administrative. Des dispositions spécifiques organisent les mesures de contrôle concernant les seuls systèmes d'information. La transposition de la directive permet donc de créer un mécanisme efficace de supervision et de contrôle sur tout le périmètre de la sécurité des activités d'importance vitale.

	l'opérateur et des travaux à exécuter. Les arrêtés concernant les entreprises nationales ou faisant appel au concours financier de l'Etat sont transmis au ministre de tutelle et au ministre de l'économie et des finances, qui sont immédiatement informés des difficultés susceptibles de se produire dans l'application de l'arrêté. **L. 1332-6-3** : A la demande du Premier ministre, les opérateurs mentionnés aux articles L. 1332-1 et L. 1332-2 soumettent leurs		sur tout support, ou procéder à la saisie de ces documents en quelques mains qu'ils se trouvent. Ils peuvent procéder, sur convocation ou sur place, aux auditions de toute personne susceptible d'apporter des éléments utiles à leurs constatations. Ils en dressent procès-verbal. Les personnes entendues procèdent elles-mêmes à sa lecture, peuvent y faire consigner leurs observations et y apposent leur signature. En cas de refus de signer le procès-verbal, mention en est faite sur celui-ci.	

	systèmes d'information à des contrôles destinés à vérifier le niveau de sécurité et le respect des règles de sécurité prévues à l'article L. 1332-6-1. Les contrôles sont effectués par l'autorité nationale de sécurité des systèmes d'information ou par des services de l'Etat désignés par le Premier ministre ou par des prestataires de service qualifiés par ce dernier. Le coût des contrôles est à la charge de l'opérateur.		Ils sont astreints au secret professionnel pour les faits, actes ou renseignements dont ils ont pu avoir connaissance en raison de leurs fonctions, dans les conditions prévues à l'article 226-13 du code pénal. Le secret professionnel ne peut leur être opposé. Les infractions et les manquements sont constatés par des procès-verbaux, qui font foi jusqu'à preuve contraire. Il est dressé procès-verbal des vérifications et visites menées en application du présent	

			article. **Article L. 1332-14** Il est interdit de faire obstacle à l'exercice des fonctions des agents habilités. L'opérateur contrôlé est tenu de coopérer avec l'autorité administrative. Les agents mentionnés à l'article L. 1332-12 peuvent constater toute action de l'opérateur d'importance vitale de nature à faire obstacle au contrôle. Le fait pour quiconque de faire obstacle aux demandes de l'autorité compétente nécessaires à	

			la recherche des manquements et à la mise en œuvre de ses pouvoirs de contrôle prévus par la présente sous-section, notamment en fournissant des renseignements incomplets ou inexacts, ou en communiquant des pièces incomplètes ou dénaturées, est puni d'une amende administrative prononcée par la commission des sanctions mentionnée à l'article L. 1332-15 dont le montant, proportionné à la gravité du manquement, ne peut excéder 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, le montant le plus élevé étant retenu. Ces dispositions ne s'appliquent pas à l'Etat et à ses établissements publics qui font l'objet d'un contrôle.	
3. Au plus tard le 17 juillet 2028, et tous les deux ans par la suite, les points de contact uniques présentent à la Commission et au groupe sur la résilience des entités critiques visé à l'article 19 un rapport de synthèse sur les notifications qu'ils ont reçues, mentionnant le nombre de notifications, la nature des incidents signalés et les mesures prises conformément à l'article 15, paragraphe 3. La Commission, en coopération	Sans objet	Sans objet pour ce qui concerne le projet de loi. Les documents type de planification destinés aux opérateurs seront détaillés dans les mesures réglementaires d'application (décret en Conseil d'Etat et arrêtés interministériels).	Sans objet	Ces dispositions concernent les Etats membres et les objectifs assignés seront déclinés en tant que de besoin par le Gouvernement.

avec le groupe sur la résilience des entités critiques, élabore un modèle commun de rapport. Les autorités compétentes peuvent utiliser, à titre volontaire, ce modèle commun de rapport aux fins de la présentation des rapports de synthèse visés au premier alinéa. 4. Chaque État membre veille à ce que son autorité compétente et son point de contact unique disposent des pouvoirs et des ressources financières, humaines et techniques nécessaires pour accomplir, de manière efficace et efficiente, les tâches qui leur sont assignées. 5. Chaque État membre veille à ce que son autorité compétente consulte, chaque fois que cela est approprié, et conformément au droit de l'Union et au droit national, les autres autorités				

nationales concernées, y compris celles chargées de la protection civile, de l'application de la loi et de la protection des données à caractère personnel, et les entités critiques et les parties intéressées concernées, et à ce qu'elle coopère avec celles-ci. 6. Chaque État membre veille à ce que son autorité compétente en vertu de la présente directive coopère et échange des informations avec les autorités compétentes en vertu de la directive (UE) 2022/2555 sur les risques, menaces et incidents en matière de cybersécurité et sur les risques, menaces et incidents non liés à la cybersécurité affectant les entités critiques, y compris en ce qui concerne les mesures pertinentes que son autorité compétente et les autorités compétentes en vertu de la directive (UE) 2022/2555				

ont prises. 7. Dans les trois mois à compter de la désignation ou de la mise en place de l'autorité compétente et du point de contact unique, chaque État membre notifie à la Commission leur identité et les tâches et responsabilités qui leur incombent en vertu de la présente directive, leurs coordonnées, ainsi que toute modification ultérieure y relative. Les États membres informent la Commission lorsqu'ils décident de désigner une autorité autre que les autorités compétentes visées au paragraphe 1, deuxième alinéa, en tant qu'autorités compétentes à l'égard des entités critiques des secteurs figurant aux points 3, 4 et 8 du tableau de l'annexe. Chaque État membre rend publique l'identité de son				

autorité compétente et de son point de contact unique. 8. La Commission met une liste des points de contact uniques à la disposition du public. **Article 10** **Soutien des États membres aux entités critiques** 1. Les États membres aident les entités critiques à renforcer leur résilience. Dans ce cadre, ils peuvent élaborer des documents d'orientation et des méthodologies, apporter leur soutien à l'organisation d'exercices visant à tester leur résilience et dispenser des conseils et des formations au personnel des entités critiques. Sans préjudice des règles applicables en matière d'aides d'État, les États membres peuvent fournir des ressources				

financières aux entités critiques, lorsque cela est nécessaire et justifié par des objectifs d'intérêt général. 2. Chaque État membre veille à ce que son autorité compétente coopère et échange des informations et des bonnes pratiques avec les entités critiques des secteurs figurant à l'annexe. 3. Les États membres facilitent le partage volontaire d'informations entre les entités critiques sur les questions couvertes par la présente directive, conformément au droit de l'Union et au droit national en matière, en particulier, d'informations classifiées et sensibles, de concurrence et de protection des données à caractère personnel.				

Article 11 **Coopération entre États membres** 1. Chaque fois que cela est approprié, les États membres se consultent mutuellement au sujet des entités critiques aux fins d'assurer l'application cohérente de la présente directive. Ces consultations ont lieu en particulier au sujet des entités critiques qui : a) utilisent des infrastructures critiques qui sont physiquement connectées entre deux États membres ou plus ; b) font partie de structures d'entreprise qui sont connectées ou liées à des entités critiques dans d'autres États membres ;				

c) ont été recensées en tant qu'entités critiques dans un État membre et fournissent des services essentiels à ou dans d'autres États membres. 2. Les consultations visées au paragraphe 1 visent à renforcer la résilience des entités critiques et, si possible, à réduire la charge administrative pesant sur celles-ci.				
Article 12 **Évaluation des risques par les entités critiques** 1. Nonobstant le délai énoncé à l'article 6, paragraphe 3, deuxième alinéa, les États membres veillent à ce que les entités critiques procèdent à une évaluation des risques dans un délai de neuf mois suivant la	Sans objet	Mesures de nature législative qui fixent une obligation pour les opérateurs désignés et qui ont un impact sur la liberté du commerce et de l'industrie, la liberté d'entreprendre et, le cas échéant, porte atteinte à la libre administration des collectivités territoriales.	**Article L. 1332-3, alinéas 1 et 2** : Les opérateurs d'importance vitale réalisent une analyse des risques de toute nature, y compris à caractère terroriste, qui pourraient perturber l'exercice de leurs activités d'importance vitale ou la	Le Gouvernement a choisi dans ce cas de procéder à la transposition directe de la directive en englobant de manière générale les risques devant être analysés par les opérateurs ainsi que les délais afférents mentionnés au 1 de l'article 12 de la directive.

réception de la notification visée à l'article 6, paragraphe 3, selon les besoins par la suite et au moins tous les quatre ans, sur la base des évaluations des risques d'États membres et d'autres sources d'informations pertinentes, afin d'évaluer tous les risques pertinents qui pourraient perturber la fourniture de leur services essentiels (ci-après dénommée «évaluation des risques d'entité critique»). 2. Les évaluations des risques d'entités critiques rendent compte de tous les risques naturels et d'origine humaine pertinents, susceptibles d'entraîner un incident, y compris ceux qui revêtent un caractère transsectoriel ou transfrontière, des accidents, des catastrophes naturelles, des urgences de santé publique et des menaces hybrides et autres		Un décret en Conseil d'Etat précisera ces mesures	sécurité de leurs infrastructures critiques, notamment des points d'importance vitale désignés par l'autorité administrative. Cette analyse est réalisée au plus tard dans un délai de neuf mois à compter de la désignation prévue au I de l'article L. 1332-2 et réévaluée au moins tous les quatre ans. **Article L. 1332-4** Les opérateurs d'importance vitale réalisent, au plus tard dans un délai de neuf mois à compter de la désignation prévue au I	Il a également été fait le choix de mentionner expressément l'analyse spécifique de dépendance à l'égard de tiers, notamment s'agissant des chaînes d'approvisionnement et des vulnérabilités pesant sur celles-ci.

menaces antagonistes, lesquelles comprennent les infractions terroristes prévues par la directive (UE) 2017/541. Une évaluation des risques d'entité critique tient compte de la mesure dans laquelle d'autres secteurs figurant à l'annexe dépendent du service essentiel fourni par l'entité critique et de la mesure dans laquelle cette entité critique dépend des services essentiels fournis par d'autres entités de ces autres secteurs, y compris s'il y a lieu, dans les États membres voisins et les pays tiers. Lorsqu'une entité critique a réalisé d'autres évaluations des risques ou établi des documents en vertu d'obligations prévues dans d'autres actes juridiques qui sont pertinents pour son évaluation des risques d'entité critique, elle peut utiliser ces			de l'article L. 1332-2, une analyse de leurs dépendances à l'égard de tiers, y compris ceux situés en dehors du territoire national, pour l'exercice de leurs activités d'importance vitale. Celle-ci comprend notamment une analyse des éventuelles vulnérabilités de leurs chaînes d'approvisionnement. Les mesures de résilience adoptées par les opérateurs d'importance vitale tiennent compte de cette analyse. Les opérateurs d'importance vitale prennent les mesures nécessaires pour garantir	

évaluations et documents pour satisfaire aux exigences énoncées dans le présent article. Dans l'exercice de ses fonctions de supervision, l'autorité compétente peut déclarer qu'une évaluation des risques existante réalisée par une entité critique qui porte sur les risques et le degré de dépendance visés au premier alinéa du présent paragraphe respecte, en tout ou en partie, les obligations prévues par le présent article.			l'application des dispositions prévues au présent chapitre.	
Article 13 **Mesures de résilience des entités critiques** 1. Les États membres veillent à ce que les entités critiques prennent des mesures techniques, des mesures de sécurité et des mesures organisationnelles appropriées et	**Article L. 1332-1** : Les opérateurs publics ou privés exploitant des établissements ou utilisant des installations et ouvrages, dont l'indisponibilité risquerait de diminuer d'une façon	Mesures de nature législative qui fixent une obligation pour les opérateurs désignés et qui ont un impact sur la liberté du commerce et de l'industrie, la liberté d'entreprendre et, le cas échéant, porte atteinte à la libre administration des	**Article L. 1332-3 :** Les opérateurs d'importance vitale réalisent une analyse des risques de toute nature, y compris à caractère terroriste, qui pourraient perturber l'exercice de leurs activités d'importance vitale ou la	Passant d'une logique de protection à une logique de résilience, le dispositif de sécurité des activités d'importance vitale, tout en étant conservé, est modernisé par les apports de la directive dont il est procédé à la transposition, ainsi que le propose le projet, au travers de

proportionnées pour garantir leur résilience, sur la base des informations pertinentes fournies par les États membres concernant l'évaluation des risques d'État membre et les résultats de l'évaluation des risques d'entité critique, y compris des mesures nécessaires pour : a) prévenir la survenance d'incidents, en tenant dûment compte de mesures de réduction des risques de catastrophe et d'adaptation au changement climatique ; b) assurer une protection physique adéquate de leurs locaux et infrastructures critiques, en prenant dûment en considération, par exemple, des clôtures, des barrières, des outils et procédures de surveillance des enceintes, et des équipements de	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. Ces établissements, installations ou ouvrages sont désignés par l'autorité administrative. **L. 1332-3 :** Les opérateurs dont un ou plusieurs	collectivités territoriales. Un décret en Conseil d'Etat précisera ces mesures	sécurité de leurs infrastructures critiques, notamment des points d'importance vitale désignés par l'autorité administrative. Cette analyse est réalisée au plus tard dans un délai de neuf mois à compter de la désignation prévue au I de l'article L. 1332-2 et réévaluée au moins tous les quatre ans. Sur le fondement de cette analyse, les opérateurs d'importance vitale adoptent des mesures de résilience techniques, opérationnelles et organisationnelles, et proportionnées, afin	plusieurs articles déclinant les différentes obligations devant se matérialiser dans des documents de planification. Le Gouvernement a donc opté pour une solution similaire à celle existante en y incluant celles des obligations complémentaires et rénovées. Il en est ainsi de l'analyse de risques, des éléments à prendre en compte pour assurer la résilience – dont la définition est simplifiée dans le projet de loi mais sans restreindre le champ de la directive (1 de l'article 13), des mesures pouvant être considérées comme équivalentes (2 de l'article 13).

détection et de contrôle des accès ; c) réagir et résister aux conséquences des incidents et les atténuer, en prenant dûment en considération la mise en œuvre de procédures et protocoles de gestion des risques et des crises et de procédures d'alerte ; d) se rétablir d'incidents, en prenant dûment en considération des mesures assurant la continuité des activités et la détermination d'autres chaînes d'approvisionnement, afin de reprendre la fourniture du service essentiel ; e) assurer une gestion adéquate de la sécurité liée au personnel, en prenant dûment en considération des mesures telles que la définition des catégories de personnel qui exerce des fonctions critiques,	établissements, installations et ouvrages sont désignés en application du présent chapitre réalisent pour chacun d'eux les mesures de protection prévues à un plan particulier de protection dressé par l'opérateur et approuvé par l'autorité administrative. Ces mesures comportent notamment des dispositions efficaces de surveillance, d'alarme et de protection matérielle. En cas de non-approbation du plan et de désaccord persistant, la décision		d'assurer la continuité des activités d'importance vitale qu'ils exercent et de sauvegarder leurs infrastructures critiques. L'analyse des risques ainsi que les mesures de résilience sont détaillées dans un document dénommé "plan de résilience opérateur" élaboré par l'opérateur, au plus tard dans un délai de dix mois à compter de la désignation prévue au I de l'article L. 1332-2, et approuvé par l'autorité administrative. Lorsque, en application d'accords internationaux	Les autres points de l'article 13 ne nécessitent pas de transposition en ce qu'ils concernent les Etats membres (4, 5 et 6) ou relèvent du domaine réglementaire (3 de l'article 13).

l'établissement de droits d'accès aux locaux, aux infrastructures critiques et aux informations sensibles, la mise en place de procédures de vérification des antécédents conformément à l'article 14, la désignation des catégories de personnes tenues de faire l'objet de telles vérifications des antécédents et la définition d'exigences et de qualifications appropriées en matière de formation ; f) sensibiliser le personnel concerné aux mesures visées aux points a) à e), en tenant dûment compte des séances de formation, du matériel d'information et des exercices. Aux fins du premier alinéa, point e), les États membres veillent à ce que les entités critiques tiennent compte du personnel des prestataires de services	est prise par l'autorité administrative. **L. 1332-6-1** : Le Premier ministre fixe les règles de sécurité nécessaires à la protection des systèmes d'information des opérateurs mentionnés aux articles L. 1332-1 et L. 1332-2 et des opérateurs publics ou privés qui participent à ces systèmes pour lesquels l'atteinte à la sécurité ou au fonctionnement risquerait de diminuer d'une façon importante le potentiel de guerre ou économique, la		régulièrement ratifiés ou approuvés, de lois ou de règlements, l'opérateur a déjà décrit dans un document particulier tout ou partie des mesures prévues au deuxième alinéa, l'autorité administrative peut décider que ce document tient lieu, pour tout ou partie, du "plan de résilience opérateur". En cas de refus de l'opérateur d'élaborer ce plan, de le modifier afin de le rendre conforme aux exigences prévues au présent article ou de le mettre en œuvre, l'autorité administrative le met en demeure de le réaliser, de le modifier ou	

extérieurs lorsqu'ils définissent les catégories de personnel qui exerce des fonctions critiques. 2. Les États membres veillent à ce que les entités critiques aient mis en place et appliquent un plan de résilience ou un ou plusieurs documents équivalents, qui décrivent les mesures prises en application du paragraphe 1. Lorsque les entités critiques ont élaboré des documents ou pris des mesures en vertu d'obligations prévues dans d'autres actes juridiques qui sont pertinents pour les mesures visées au paragraphe 1, elles peuvent utiliser ces documents et mesures pour satisfaire aux exigences énoncées dans le présent article. Dans l'exercice de ses fonctions de supervision, l'autorité compétente peut déclarer que des mesures existantes de renforcement de la	sécurité ou la capacité de survie de la Nation ou pourrait présenter un danger grave pour la population. Ces opérateurs sont tenus d'appliquer ces règles à leurs frais. Les règles mentionnées au premier alinéa peuvent notamment prescrire que les opérateurs mettent en œuvre des systèmes qualifiés de détection des événements susceptibles d'affecter la sécurité de leurs systèmes d'information. Ces systèmes de détection sont exploités sur le territoire national par des prestataires de		de le mettre en œuvre dans un délai qu'elle fixe et qui ne saurait être inférieur à un mois. L'autorité administrative peut assortir cette mise en demeure d'une astreinte d'un montant maximal de 5 000 euros par jour de retard. L'astreinte peut également être prononcée à tout moment, après l'expiration du délai imparti par la mise en demeure, s'il n'y a pas été satisfait, après que l'intéressé a été invité à présenter ses observations.	

résilience prises par une entité critique qui portent, de manière appropriée et proportionnée, sur les mesures techniques, les mesures de sécurité et les mesures organisationnelles visées au paragraphe 1 respectent, en tout ou en partie, les obligations prévues par le présent article. 3. Les États membres veillent à ce que chaque entité critique désigne un agent de liaison ou une personne ayant une fonction équivalente en tant que point de contact avec les autorités compétentes. 4. À la demande de l'État membre qui a déterminé l'entité critique et avec l'accord de l'entité critique concernée, la Commission organise des missions de conseil, conformément aux modalités	service qualifiés en matière de sécurité de systèmes d'information, par l'autorité nationale de sécurité des systèmes d'information ou par d'autres services de l'Etat désignés par le Premier ministre. Les qualifications des systèmes de détection et des prestataires de service exploitant ces systèmes sont délivrées par le Premier ministre.		Les opérateurs mentionnés au 2° du I de l'article L. 1332-2 mettent en œuvre ces mesures de résilience sous réserve des dispositions du titre Ier du livre V du code de l'environnement et des dispositions du chapitre III du titre IX du livre V du même code. Un décret en Conseil d'Etat précise la nature des mesures de résilience pour chaque catégorie d'opérateur d'importance vitale mentionné au I de l'article L. 1332-2.	

prévues à l'article 18, paragraphes 6, 8 et 9, afin de conseiller l'entité critique concernée en vue du respect des obligations qui lui incombent en vertu du chapitre III. La mission de conseil communique ses conclusions à la Commission, audit État membre et à l'entité critique concernée. 5. Après consultation du groupe sur la résilience des entités critiques visé à l'article 19, la Commission adopte des lignes directrices non contraignantes afin de préciser davantage les mesures techniques, les mesures de sécurité et les mesures organisationnelles qui peuvent être prises en vertu du paragraphe 1 du présent article. 6. La Commission adopte des actes d'exécution afin d'établir			**Article L. 1332-4** Les opérateurs d'importance vitale réalisent, au plus tard dans un délai de neuf mois à compter de la désignation prévue au I de l'article L. 1332-2, une analyse de leurs dépendances à l'égard de tiers, y compris ceux situés en dehors du territoire national, pour l'exercice de leurs activités d'importance vitale. Celle-ci comprend notamment une analyse des éventuelles vulnérabilités de leurs chaînes d'approvisionnement. Les mesures de résilience adoptées par les opérateurs d'importance vitale tiennent compte de	

les spécifications techniques et méthodologiques nécessaires relatives à l'application des mesures visées au paragraphe 1 du présent article. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 24, paragraphe 2.			cette analyse. Les opérateurs d'importance vitale prennent les mesures nécessaires pour garantir l'application des dispositions prévues au présent chapitre. **Article L. 1332-5 :** Les opérateurs dont un ou plusieurs points d'importance vitale sont désignés en application du présent chapitre réalisent pour chacun d'eux un document dénommé "plan particulier de résilience" détaillant les mesures de protection et de résilience	

			les concernant. Ces mesures comportent notamment des dispositions efficaces de surveillance, d'alarme, de protection matérielle et de conditions d'accès. Le plan est approuvé par l'autorité administrative. Lorsque, en application d'accords internationaux régulièrement ratifiés ou approuvés, de lois ou de règlements, un point d'importance vitale fait déjà l'objet de mesures de protection suffisantes décrites dans un document particulier, l'autorité administrative peut décider que ce	

			document tient lieu de “plan particulier de résilience”. En cas de refus de l’opérateur d’élaborer ce plan, de le modifier afin de le rendre conforme aux exigences prévues aux alinéas précédents ou de le mettre en œuvre, l’autorité administrative le met en demeure de le réaliser, de le modifier ou de le mettre en œuvre dans un délai qu’elle fixe et qui ne saurait être inférieur à un mois. L’autorité administrative peut assortir cette mise en demeure d’une astreinte d’un montant	

			maximal de 5 000 euros par jour de retard. L'astreinte peut également être prononcée à tout moment, après l'expiration du délai imparti par la mise en demeure, s'il n'y a pas été satisfait, après que l'opérateur concerné a été invité à présenter ses observations.	
Article 14 **Vérification des antécédents** 1. Les États membres précisent les conditions dans lesquelles une entité critique est autorisée,	**Article L. 1332-2-1 :** L'accès à tout ou partie des établissements, installations et ouvrages désignés en	Mesures de nature législative compte tenu des atteintes portées aux droits des personnes concernées. Un décret en Conseil d'Etat précisera ces	**Article L. 1332-6** : Avant d'accorder une autorisation d'accès physique ou à distance à ses points d'importance vitale et systèmes	Des dispositions relatives aux enquêtes administratives de sécurité existant déjà avant l'adoption de la directive, il a été fait le choix de transposer l'article 14 en

dans des cas dûment motivés et compte tenu de l'évaluation des risques d'État membre, à présenter des demandes de vérification des antécédents des personnes : a) qui occupent des fonctions sensibles au sein de l'entité critique ou au bénéfice de celle-ci, notamment en ce qui concerne la résilience de l'entité critique ; b) qui sont autorisées à avoir un accès direct ou à distance aux locaux et aux systèmes d'information ou de contrôle de l'entité critique, y compris en lien avec sa sécurité ; c) dont le recrutement est envisagé à des postes répondant aux critères énoncés au point a) ou b). 2. Les demandes visées au	application du présent chapitre est autorisé par l'opérateur qui peut demander l'avis de l'autorité administrative compétente dans les conditions et selon les modalités définies par décret en Conseil d'Etat. L'avis est rendu à la suite d'une enquête administrative qui peut donner lieu à la consultation du bulletin n° 2 du casier judiciaire et de traitements automatisés de données à caractère personnel relevant de l'article 31 de la loi n° 78-17 du 6 janvier 1978 relative à	mesures notamment concernant la détermination des catégories de personnes à envisager.	d'information d'importance vitale, l'opérateur d'importance vitale peut demander l'avis de l'autorité administrative compétente dans les conditions prévues par l'article L. 114-1 du code de la sécurité intérieure, selon des modalités fixées par décret en Conseil d'Etat, lorsqu'il estime nécessaire de s'assurer que le comportement de la personne devant faire l'objet de l'autorisation d'accès n'est pas de nature à porter atteinte à l'exercice d'une activité d'importance vitale ou à la sécurité d'une infrastructure critique.	prévoyant des mesures conformes aux dispositions du code de la sécurité intérieure tout en élargissant le champ aux accès à distance et aux fonctions sensibles qui sont prévus par l'article 14 et qui ne sont pas inclus actuellement Par ailleurs, ainsi que proposé par le Conseil d'Etat dans son avis portant sur le projet de loi relatif aux jeux Olympiques et Paralympiques de 2024 et portant diverses autres dispositions (n° 406.383 du 15 décembre 2022, §31), le Gouvernement a retenu un avis conforme de l'autorité administrative compétente dans le seul cas d'un avis négatif sollicité par un opérateur privé.

paragraphe 1 du présent article sont évaluées dans un délai raisonnable et traitées conformément au droit national et aux procédures nationales, ainsi qu'au droit de l'Union pertinent et applicable, y compris le règlement (UE) 2016/679 et la directive (UE) 2016/680 du Parlement européen et du Conseil (37). Les vérifications des antécédents sont proportionnées et strictement limitées à ce qui est nécessaire. Elles sont effectuées dans le seul but d'évaluer un risque potentiel pour la sécurité de l'entité critique concernée. 3. À tout le moins, une vérification des antécédents visée au paragraphe 1 : a) corrobore l'identité de la personne qui fait l'objet d'une demande de vérification des	l'informatique, aux fichiers et aux libertés, à l'exception des fichiers d'identification. La personne concernée est informée de l'enquête administrative dont elle fait l'objet.		Il peut également solliciter cet avis avant le recrutement ou l'affectation d'une personne à un poste pour l'exercice duquel il est nécessaire d'avoir accès aux points d'importance vitale ou aux systèmes d'information d'importance vitale ou qui implique l'occupation de fonctions sensibles. Les fonctions sensibles sont celles qui sont indispensables à la réalisation d'une activité d'importance vitale ou dont l'occupation expose l'opérateur à des vulnérabilités. Elles sont	Il a également été précisé la nécessité pour l'opérateur de justifier, au travers de ses différents documents de planification, les demandes d'enquête afin de garantir les droits des personnes concernées, lesquelles doivent en outre être informées.

antécédents ; b) vérifie les casiers judiciaires de cette personne en ce qui concerne des infractions qui seraient pertinentes pour un poste déterminé ; Lors de la vérification des antécédents, les États membres, recourent au système européen d'information sur les casiers judiciaires conformément aux procédures prévues dans la décision-cadre 2009/315/JAI et, si cela est pertinent et applicable, dans le règlement (UE) 2019/816, aux fins de l'obtention des informations issues des casiers judiciaires détenus par d'autres États membres. Les autorités centrales visées à l'article 3, paragraphe 1, de la décision-cadre 2009/315/JAI et à l'article 3, point 5, du règlement (UE)			énumérées par l'opérateur dans le plan de résilience prévu au quatrième alinéa de l'article L. 1332-3 en tenant compte, le cas échéant, de critères déterminés par l'autorité administrative en fonction du secteur d'activité de l'opérateur. Les cas dans lesquels les accès physique ou à distance peuvent justifier la demande d'avis sont précisés par l'opérateur dans le plan de résilience prévu au quatrième alinéa de l'article L. 1332-3 et, le cas échéant, dans le plan particulier de résilience prévu à l'article L. 1332-5 en	

2019/816 répondent aux demandes d'informations dans un délai de dix jours ouvrables à compter de la date de réception de la demande conformément à l'article 8, paragraphe 1, de la décision-cadre 2009/315/JAI.			tenant compte des vulnérabilités à des actes de malveillance. La personne concernée est informée de l'enquête administrative dont elle fait l'objet. En cas d'avis défavorable de l'autorité administrative, l'opérateur d'importance vitale est tenu de refuser l'autorisation s'il est une personne morale de droit privé. Un avis défavorable ne peut être émis que s'il ressort de l'enquête administrative que le comportement de la personne ayant fait l'objet de l'enquête est	

			de nature à porter atteinte à l'exercice d'une activité d'importance vitale ou à la sécurité d'une infrastructure critique	
Article 15 **Notification d'incidents** 1. Les États membres veillent à ce que les entités critiques notifient sans retard injustifié à l'autorité compétente les incidents qui perturbent ou sont susceptibles de perturber de manière importante la fourniture de services essentiels. Les États membres veillent à ce que, sauf à être dans l'incapacité de le faire pour des raisons opérationnelles, les entités critiques présentent une première notification au plus tard 24 heures après avoir pris	Sans objet	Mesures de nature législative compte tenu des sujétions imposées aux opérateurs dont le défaut pourrait être sanctionné. Un décret en Conseil d'Etat précisera les modalités d'application.	**Article L. 1332-7** Les opérateurs d'importance vitale désignés au titre du 1° du I de l'article L. 1332-2 notifient à l'autorité administrative tout incident susceptible de compromettre la continuité de ses activités d'importance vitale dans un délai prévu par décret en Conseil d'Etat. L'autorité administrative informe le public de cet incident lorsqu'elle estime qu'il est dans	Le Gouvernement a fait le choix de transposer le 1 de l'article 15 de la directive en inscrivant dans le projet de loi les seuls éléments relevant de l'article 34 de la Constitution. Il a simplement été retenu, comme pour l'ensemble du projet de loi, de conserver les notions déjà connues qui sont en tout état de cause compatibles avec les objectifs de la directive.

connaissance d'un incident, suivie, s'il y a lieu, d'un rapport détaillé au plus tard un mois après. Afin de déterminer l'importance de la perturbation, les paramètres suivants sont, en particulier, pris en compte : a) le nombre et la proportion d'utilisateurs affectés par la perturbation ; b) la durée de la perturbation ; c) la zone géographique concernée par la perturbation, en tenant compte de son éventuel isolement géographique. Lorsqu'un incident a ou pourrait avoir un impact important sur la continuité de la fourniture de services essentiels à ou dans six États membres ou plus, les autorités compétentes des États membres affectés par l'incident notifient ledit incident à la			l'intérêt général de le faire	

Commission.				
2. Les notifications visées au paragraphe 1, premier alinéa, comprennent toutes les informations disponibles nécessaires pour permettre à l'autorité compétente de comprendre la nature, la cause et les conséquences possibles de l'incident, y compris toute information disponible nécessaire pour déterminer tout impact transfrontière de l'incident. Ces notifications n'ont pas pour effet de soumettre les entités critiques à une responsabilité accrue.		Un décret en Conseil d'Etat précisera les modalités d'application.	Sans objet	Le décret précisera les conditions et délais de la notification d'incidents.
3. Sur la base des informations fournies par une entité critique dans une notification visée au paragraphe 1, l'autorité compétente concernée, par		Sans objet	Sans objet	Ces dispositions concernent les Etats membres mais seront mises en œuvre par le Gouvernement sans qu'une base législative soit

l'intermédiaire du point de contact unique, informe le point de contact unique des autres États membres affectés lorsque l'incident a ou pourrait avoir un impact important sur les entités critiques et sur la continuité de la fourniture de services essentiels à ou dans un ou plusieurs autres États membres. Les points de contact uniques qui envoient et reçoivent des informations en vertu du premier alinéa traitent ces informations, conformément au droit de l'Union ou au droit national, de manière à en respecter la confidentialité et à préserver la sécurité et les intérêts commerciaux de l'entité critique concernée. 4. Dès que possible après la réception d'une notification visée au paragraphe 1, l'autorité				nécessaire

compétente concernée fournit à l'entité critique concernée des informations de suivi pertinentes, y compris des informations qui pourraient aider ladite entité critique à réagir efficacement à l'incident en question. Les États membres informent le public lorsqu'ils estiment qu'il serait dans l'intérêt général de le faire.				
Article 16 **Normes** Afin de favoriser la mise en œuvre convergente de la présente directive, les États membres encouragent, lorsque c'est utile et sans imposer ni créer de discriminations en faveur de l'utilisation d'un type particulier de technologie, le recours à des normes et des	Sans objet	Sans objet	Sans objet	Sans objet

spécifications techniques européennes et internationales pertinentes pour les mesures de sécurité et les mesures de résilience applicables aux entités critiques.				
Article 17 **Recensement des entités critiques d'importance européenne particulière** 1. Une entité est considérée comme une entité critique d'importance européenne particulière lorsqu'elle : a) a été désignée en tant qu'entité critique conformément à l'article 6, paragraphe 1 ; b) fournit les mêmes services	Sans objet	Mesures de nature législative compte tenu des sujétions imposées aux opérateurs dont le défaut pourrait être sanctionné. Un décret en Conseil d'Etat précisera les modalités d'application	**Article L. 1332-2, I, 1°** Sont désignés opérateurs d'importance vitale par l'autorité administrative : 1° Les opérateurs publics ou privés exerçant, au moyen d'infrastructures critiques situées sur le territoire national, une activité d'importance vitale ;	Afin de maintenir son dispositif actuel de sécurité des activités d'importance vitale, ainsi que détaillé précédemment, le Gouvernement a donc privilégié l'option de transposer fidèlement l'article 17 en prévoyant les mesures concernant les seules entités critiques d'importance européenne particulière (ECIEP) : - identification et recensement des ECIEP à partir des informations

essentiels ou des services essentiels similaires à ou dans six États membres ou plus; et c) elle a fait l'objet d'une notification conformément au paragraphe 3 du présent article. 2. Les États membres veillent à ce qu'une entité critique, à la suite de la notification visée à l'article 6, paragraphe 3, informe son autorité compétente lorsqu'elle fournit des services essentiels à ou dans six États membres ou plus. En pareil cas, les États membres veillent à ce que l'entité critique informe son autorité compétente au sujet des services essentiels qu'elle fournit à ou dans ces États membres et au sujet des États membres auxquels ou dans lesquels elle fournit ces services essentiels. Les États membres notifient à la Commission, sans			L'autorité administrative précise, le cas échéant, dans l'acte de désignation de l'opérateur d'importance vitale, l'activité ou la liste des activités d'importance vitale exercées par l'opérateur qui constituent des services essentiels au fonctionnement du marché intérieur de l'Union européenne définis par le règlement délégué (UE) 2023/2450 de la Commission du 25 juillet 2023 complétant la directive (UE) 2022/2557 du Parlement européen et du Conseil en établissant une liste de services essentiels et qui, à ce titre, doivent être regardés comme des entités critiques au sens	transmises par les OIV fournissant des services essentiels tels que déterminés dans les conditions mentionnées au 1° du I de l'article L. 1332-2 (cf détails supra sur la transposition de l'objectif de recensement des entités critiques prévu à l'article 6 de la directive) ; - exclusion des domaines « régaliens » non couverts par la directive ; - conséquences sur la mission de conseil de la Commission (article 18 de la directive).

retard injustifié, l'identité de ces entités critiques et les informations qu'elles fournissent au titre du présent paragraphe. La Commission consulte l'autorité compétente de l'État membre qui a déterminé une entité critique visée au premier alinéa, l'autorité compétente des autres États membres concernés et l'entité critique en question. Lors de ces consultations, chaque État membre informe la Commission lorsqu'il estime que les services qui sont fournis audit État membre par l'entité critique sont des services essentiels. 3. Lorsque la Commission établit, sur la base des consultations visées au paragraphe 2 du présent article, que l'entité critique concernée fournit des services essentiels à			de cette directive ; **Article L. 1332-8** Les opérateurs d'importance vitale qui fournissent les mêmes services essentiels ou des services essentiels similaires dans au moins six Etats membres en informent l'autorité administrative au plus tard en même temps que la présentation pour approbation du plan de résilience prévu au troisième alinéa de l'article L. 1332-3. Ces opérateurs sont identifiés comme entités critiques d'importance	

ou dans six États membres ou plus, la Commission notifie à ladite entité critique, par l'intermédiaire de son autorité compétente, qu'elle est considérée comme une entité critique d'importance européenne particulière et l'informe des obligations qui lui incombent en vertu du présent chapitre et de la date à partir de laquelle ces obligations lui sont applicables. Une fois que la Commission informe l'autorité compétente de sa décision de considérer une entité critique comme une entité critique d'importance européenne particulière, l'autorité compétente transmet ladite notification à ladite entité critique sans retard injustifié. 4. Le présent chapitre s'applique à l'entité critique d'importance européenne			européenne particulière de l'opérateur dans les conditions prévues à l'article 17 de la directive (UE) 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. Les opérateurs qui exercent des activités dans les domaines de la sécurité nationale, de la sécurité publique, de la défense, du nucléaire ou de la répression pénale, ou qui fournissent des services exclusivement destinés aux entités de l'administration publique exerçant dans ces	

particulière concernée à compter de la date de réception de la notification visée au paragraphe 3 du présent article. **Article 18** **Missions de conseil** 1. À la demande de l'État membre qui a désigné une entité critique d'importance européenne particulière en tant qu'entité critique en vertu de l'article 6, paragraphe 1, la Commission organise une mission de conseil afin d'évaluer les mesures mises en place par ladite entité pour satisfaire aux obligations qui lui incombent en vertu du chapitre III. 2. De sa propre initiative ou à la demande d'un ou de plusieurs États membres auxquels ou dans lesquels le service essentiel est fourni et à condition que l'État			domaines, peuvent être exonérés par l'autorité administrative de tout ou partie des obligations mentionnées à la présente sous-section, dans des conditions prévues par décret en Conseil d'Etat. **Article L. 1332-9** Lorsque l'opérateur a été désigné par la Commission européenne comme entité critique d'importance européenne particulière il peut, avec l'accord de l'autorité administrative compétente, faire l'objet d'une mission de conseil au titre de laquelle il doit garantir l'accès aux informations, systèmes et installations relatifs à la	

membre qui a désigné une entité critique d'importance européenne particulière en tant qu'entité critique en vertu de l'article 6, paragraphe 1, y consente, la Commission organise une mission de conseil visée au paragraphe 1. 3. Sur demande motivée de la Commission ou d'un ou de plusieurs des États membres auxquels ou dans lesquels le service essentiel est fourni, l'État membre qui a désigné une entité critique d'importance européenne particulière en tant qu'entité critique en vertu de l'article 6, paragraphe 1, communique à la Commission ce qui suit: a) les éléments pertinents de l'évaluation des risques d'entité critique; b) une liste des mesures			fourniture de leurs services essentiels qui sont nécessaires à l'exécution de cette mission de conseil, dans le respect des secrets protégés par la loi. Sur le fondement des conclusions de la mission de conseil, l'opérateur se voit communiquer par la Commission européenne un avis sur le respect de ses obligations et, le cas échéant, sur les mesures qui pourraient être prises pour améliorer sa résilience.	

pertinentes prises conformément à l'article 13; c) toute mesure de supervision ou d'exécution, y compris des évaluations du respect des obligations qui ont été faites ou des injonctions qui ont été émises, prise par son autorité compétente en vertu des articles 21 et 22 à l'égard de ladite entité critique. 4. La mission de conseil communique ses conclusions à la Commission, à l'État membre qui a désigné une entité critique d'importance européenne particulière en tant qu'entité critique en vertu de l'article 6, paragraphe 1, aux États membres auxquels ou dans lesquels le service essentiel est fourni et à l'entité critique concernée, dans un délai de trois mois à compter de la fin de la				

mission de conseil. Les États membres auxquels ou dans lesquels le service essentiel est fourni analysent le rapport visé au premier alinéa et, lorsque cela est nécessaire, conseillent la Commission quant à la question du respect par l'entité critique d'importance européenne particulière concernée des obligations qui lui incombent en vertu du chapitre III et, s'il y a lieu, quant aux mesures qui pourraient être prises pour améliorer la résilience de ladite entité critique. Sur la base des conseils visés au deuxième alinéa du présent paragraphe, la Commission communique à l'État membre qui a désigné une entité critique d'importance européenne particulière en tant qu'entité critique en vertu de l'article 6,				

paragraphe 1, aux États membres auxquels ou dans lesquels le service essentiel est fourni et à ladite entité critique son avis quant à la question du respect par ladite entité critique des obligations qui lui incombent en vertu du chapitre III et, le cas échéant, quant aux mesures qui pourraient être prises pour améliorer la résilience de ladite entité critique. L'État membre qui a désigné une entité critique d'importance européenne particulière en tant qu'entité critique en vertu de l'article 6, paragraphe 1, veille à ce que son autorité compétente et l'entité critique concernée tiennent compte de l'avis visé au troisième alinéa du présent paragraphe, et fournit à la Commission et aux États membres auxquels ou dans				

lesquels le service essentiel est fourni des informations sur les mesures qu'il a adoptées à la suite de cet avis. 5. Chaque mission de conseil est composée d'experts de l'État membre dans lequel se situe l'entité critique d'importance européenne particulière, d'experts des États membres auxquels ou dans lesquels le service essentiel est fourni et de représentants de la Commission. Ces États membres peuvent proposer des candidats à la participation à une mission de conseil. À la suite d'une consultation de l'État membre qui a désigné une entité critique d'importance européenne particulière en tant qu'entité critique en vertu de l'article 6, paragraphe 1, la Commission sélectionne et nomme les membres de chaque mission de				

conseil sur la base de leurs compétences professionnelles et en veillant, lorsque cela est possible, à une représentation géographique équilibrée de tous ces États membres. Chaque fois que cela est nécessaire, les membres de la mission de conseil disposent d'une habilitation de sécurité en cours de validité et au niveau approprié. La Commission prend en charge les coûts liés à la participation à des missions de conseil. La Commission organise le programme de chaque mission de conseil, en concertation avec les membres de la mission de conseil en question et en accord avec l'État membre qui a désigné une entité critique d'importance européenne particulière en tant qu'entité critique en vertu de l'article 6,				

paragraphe 1. 6. La Commission adopte un acte d'exécution établissant les règles relatives aux modalités de procédure pour les demandes d'organisation de missions de conseil, le traitement de ces demandes, la conduite et les rapports des missions de conseil et pour le traitement de la communication de l'avis de la Commission visé au paragraphe 4, troisième alinéa, et des mesures prises, en tenant dûment compte de la confidentialité et du caractère commercial sensible des informations concernées. Cet acte d'exécution est adopté en conformité avec la procédure d'examen visée à l'article 24, paragraphe 2. 7. Les États membres veillent à ce que les entités critiques d'importance européenne				

particulière accordent aux missions de conseil l'accès aux informations, systèmes et installations relatifs à la fourniture de leurs services essentiels nécessaires à l'exécution de la mission de conseil concernée. 8. Les missions de conseil sont menées dans le respect du droit national applicable de l'État membre dans lequel elles ont lieu, en respectant la responsabilité de cet État membre en matière de sécurité nationale et la protection de ses intérêts dans le domaine de la sécurité. 9. Lorsqu'elle organise des missions de conseil, la Commission tient compte des rapports de toute inspection qu'elle a effectuée en vertu des règlements (CE) no 725/2004 et				

(CE) no 300/2008, ainsi que des rapports de tout suivi qu'elle a effectué en vertu de la directive 2005/65/CE à l'égard de l'entité critique concernée. 10. La Commission informe le groupe sur la résilience des entités critiques visé à l'article 19 chaque fois qu'une mission de conseil est organisée. L'État membre dans lequel la mission de conseil a été menée et la Commission informent également le groupe sur la résilience des entités critiques des principales conclusions de la mission de conseil et des enseignements tirés en vue de favoriser l'apprentissage mutuel				
Article 19 **Groupe sur la résilience des entités critiques** 1. Un groupe sur la résilience	Sans objet	Sans objet	Sans objet	Ces dispositions concernent les Etats membres.

des entités critiques est institué. Le groupe sur la résilience des entités critiques soutient la Commission et facilite la coopération entre les États membres et l'échange d'informations sur les questions relatives à la présente directive. 2. Le groupe sur la résilience des entités critiques est composé de représentants des États membres et de la Commission qui, s'il y a lieu, disposent d'une habilitation de sécurité. Lorsque cela est pertinent pour l'exécution de ses tâches, le groupe sur la résilience des entités critiques peut inviter des parties prenantes concernées à participer à ses travaux. Lorsque le Parlement européen le demande, la Commission peut inviter des experts du Parlement européen à assister aux réunions du groupe sur la résilience des entités critiques. Le représentant de la Commission préside le groupe				

sur la résilience des entités critiques. 3. Le groupe sur la résilience des entités critiques est chargé des tâches suivantes : a) soutenir la Commission pour ce qui est d'aider les États membres à renforcer leur capacité à contribuer à garantir la résilience des entités critiques conformément à la présente directive ; b) analyser les stratégies afin de recenser les bonnes pratiques en ce qui concerne les stratégies ; c) faciliter l'échange de bonnes pratiques concernant le recensement des entités critiques par les États membres en vertu de l'article 6, paragraphe 1, y compris pour ce qui est des dépendances transfrontières et transsectorielles et en ce qui concerne les risques et incidents ; d) s'il y a lieu, contribuer, sur les				

questions relatives à la présente directive, aux documents relatifs à la résilience au niveau de l'Union ; e) contribuer à l'élaboration des lignes directrices visées à l'article 7, paragraphe 3, et à l'article 13, paragraphe 5, et, sur demande, de tout acte délégué ou de tout acte d'exécution adopté en vertu de la présente directive ; f) analyser les rapports de synthèse visés à l'article 9, paragraphe 3, en vue de promouvoir le partage des bonnes pratiques concernant les mesures prises conformément à l'article 15, paragraphe 3 ; g) échanger les bonnes pratiques concernant la notification d'incidents visée à l'article 15 ; h) examiner les rapports de synthèse des missions de conseil et les enseignements tirés conformément à l'article 18,				

paragraphe 10 ; i) échanger des informations et les bonnes pratiques en matière d'innovation, de recherche et de développement concernant la résilience des entités critiques conformément à la présente directive ; j) s'il y a lieu, procéder à des échanges d'informations sur des questions relatives à la résilience des entités critiques avec les institutions, organes et organismes de l'Union concernés. 4. Au plus tard le 17 janvier 2025, puis tous les deux ans, le groupe sur la résilience des entités critiques établit un programme de travail prévoyant les actions à entreprendre pour réaliser ses objectifs et ses tâches. Ce programme de travail est cohérent avec les exigences et les objectifs de la présente directive.				

5. Le groupe sur la résilience des entités critiques se réunit régulièrement et en tout état de cause au moins une fois par an avec le groupe de coopération institué en vertu de la directive (UE) 2022/2555 afin de promouvoir et de faciliter la coopération et l'échange d'informations. 6. La Commission peut adopter des actes d'exécution fixant les modalités de procédure nécessaires au fonctionnement du groupe sur la résilience des entités critiques, dans le respect de l'article 1er, paragraphe 4. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 24, paragraphe 2. 7. La Commission remet au groupe sur la résilience des entités critiques un rapport de synthèse concernant les informations communiquées par les États membres en vertu de l'article 4, paragraphe 3, et de				

l'article 5, paragraphe 4, au plus tard le 17 janvier 2027, puis chaque fois que cela est nécessaire et au moins tous les quatre ans. **Article 20** **Soutien de la Commission aux autorités compétentes et aux entités critiques** 1. La Commission aide, s'il y a lieu, les États membres et les entités critiques à respecter les obligations qui leur incombent en vertu de la présente directive. La Commission élabore une vue d'ensemble, au niveau de l'Union, des risques transfrontières et transsectoriels pesant sur la fourniture de services essentiels, organise les missions de conseil visées à l'article 13, paragraphe 4, et à l'article 18, et facilite l'échange d'informations entre États membres et experts dans				

l'ensemble de l'Union. 2. La Commission complète les activités des États membres visées à l'article 10 en élaborant des bonnes pratiques, des documents d'orientation et des méthodes, et des activités de formation et des exercices transfrontières pour tester la résilience des entités critiques. 3. La Commission informe les États membres des ressources financières à leur disposition au niveau de l'Union pour renforcer la résilience des entités critiques.				
Article 21 **Supervision et exécution** 1. Afin d'évaluer le respect des obligations découlant de la présente directive par les entités qu'ils ont recensées en tant qu'entités critiques en vertu de	**Article L. 1332-3, alinéa 2** : (…) En cas de non-approbation du plan et de désaccord persistant, la décision est prise par l'autorité	Normes de nature législative s'agissant de mesures imposées aux opérateurs qui portent nécessairement atteinte à la liberté d'entreprendre et à la liberté du commerce et de l'industrie.	**Article L. 1332-3, alinéas 6 à 8** : (…) En cas de refus de l'opérateur d'élaborer ce plan, de le modifier afin de le rendre conforme aux exigences prévues au présent article ou de le	Le Gouvernement, en complément des observations concernant l'article 9 de la directive, entend préciser que les dispositions envisagées le projet de loi transposent concrètement les 1 et 2 de l'article 21 en confiant aux

l'article 6, paragraphe 1, de la présente directive, les États membres veillent à ce que les autorités compétentes disposent des pouvoirs et des moyens nécessaires pour : a) procéder à des inspections sur place de l'infrastructure critique et des locaux utilisés par l'entité critique pour fournir ses services essentiels et à la supervision à distance des mesures prises par les entités critiques conformément à l'article 13 ; b) effectuer ou ordonner des audits portant sur ces entités critiques. 2. Les États membres veillent à ce que les autorités compétentes disposent des pouvoirs et des moyens pour exiger que, lorsque l'exécution des tâches qui leur incombent en vertu de la présente directive le requiert, les	**Article L. 1332-4** : En cas de refus des opérateurs de préparer leur plan particulier de protection, l'autorité administrative met, par arrêtés, les chefs d'établissements ou d'entreprises assujettis en demeure de l'établir dans le délai qu'elle fixe. **Article L. 1332-5** : Le plan de protection établi dans les conditions prévues à l'article L. 1332-4, l'autorité administrative met, par arrêtés, les chefs	Sont également de nature législative les normes relatives aux mesures de supervision des opérateurs portant sur les obligations fixées par la loi et de sanction pour méconnaissance de ces dispositions. L'ensemble de ces normes sera précisé par décret en Conseil d'Etat	mettre en œuvre, l'autorité administrative le met en demeure de le réaliser, de le modifier ou de le mettre en œuvre dans un délai qu'elle fixe et qui ne saurait être inférieur à un mois. L'autorité administrative peut assortir cette mise en demeure d'une astreinte d'un montant maximal de 5 000 euros par jour de retard. L'astreinte peut également être prononcée à tout moment, après l'expiration du délai imparti par la mise en demeure, s'il n'y a pas été satisfait, après que	autorités administratives compétentes les prérogatives nécessaires afin de contrôler, au besoin sur place, les opérateurs. Les mesures spécifiques concernant les opérateurs relevant de la directive « NIS 2 » sont plus précisément détaillées dans le titre II du projet de loi, le titre Ier évoquant: - les obligations « cyber » applicables aux opérateurs désignés (L. 1332-11, I), - la compétence exclusive des agents de contrôle « cyber » dans le domaine qui les concerne (L. 1332-12). Le 3 de l'article 21 est transposé dans le projet de loi aux articles prévoyant

entités en vertu de la directive (UE) 2022/2555 que les États membres ont recensées en tant qu'entités critiques en vertu de la présente directive fournissent, dans un délai raisonnable fixé par ces autorités : a) les informations nécessaires pour évaluer si les mesures prises par ces entités pour garantir leur résilience satisfont aux exigences énoncées à l'article 13 ; b) la preuve de la mise en œuvre effective de ces mesures, y compris les résultats d'un audit effectué par un auditeur indépendant et qualifié sélectionné par ladite entité et effectué à ses frais. Lorsqu'elles requièrent ces informations, les autorités compétentes mentionnent la finalité de la demande et	d'établissements ou d'entreprises en demeure de le réaliser dans le délai qu'elle fixe. **Article L. 1332-6** : Les arrêtés de mise en demeure prévus aux articles L. 1332-4 et L. 1332-5 fixent un délai qui ne peut être inférieur à un mois, et qui est déterminé en tenant compte des conditions de fonctionnement de l'opérateur et des travaux à exécuter. Les arrêtés concernant les entreprises nationales ou faisant appel au concours		l'intéressé a été invité à présenter ses observations **Article L. 1332-5, alinéas 4 à 6** : (…) En cas de refus de l'opérateur d'élaborer ce plan, de le modifier afin de le rendre conforme aux exigences prévues aux alinéas précédents ou de le mettre en œuvre, l'autorité administrative le met en demeure de le réaliser, de le modifier ou de le mettre en œuvre dans un délai qu'elle fixe et qui ne saurait être inférieur à un mois. L'autorité administrative	des mécanismes de mise en demeure avec astreinte d'élaborer et d'appliquer les documents de planification (L. 1332-3 et L. 1332-5), l'astreinte n'étant pas dans ce cas une sanction administrative ayant un caractère punitif mais une mesure de police administrative en vue de faire cesser le trouble à la sécurité publique induit par l'absence de mise en œuvre de mesures de résilience par des opérateurs d'importance vitale. L'ensemble des garanties rendues nécessaires au 4 de l'article 21 ont bien été prises en compte et établies par le Gouvernement dans le projet.

précisent les informations exigées. 3. Sans préjudice de la possibilité d'imposer des sanctions conformément à l'article 22, les autorités compétentes peuvent, à la suite des mesures de supervision visées au paragraphe 1 du présent article ou de l'évaluation des informations visées au paragraphe 2 du présent article, enjoindre aux entités critiques concernées de prendre les mesures nécessaires et proportionnées pour remédier à toute violation constatée de la présente directive, dans un délai raisonnable fixé par lesdites autorités, et de leur fournir des informations sur les mesures prises. Ces injonctions tiennent compte, notamment, de la gravité de la violation.	financier de l'Etat sont transmis au ministre de tutelle et au ministre de l'économie et des finances, qui sont immédiatement informés des difficultés susceptibles de se produire dans l'application de l'arrêté. **Article L. 1332-6-3 :** A la demande du Premier ministre, les opérateurs mentionnés aux articles L. 1332-1 et L. 1332-2 soumettent leurs systèmes d'information à des contrôles destinés à vérifier le niveau de sécurité et le respect		peut assortir cette mise en demeure d'une astreinte d'un montant maximal de 5 000 euros par jour de retard. L'astreinte peut également être prononcée à tout moment, après l'expiration du délai imparti par la mise en demeure, s'il n'y a pas été satisfait, après que l'opérateur concerné a été invité à présenter ses observations **Article L. 1332-11, I** : Pour gérer les risques qui menacent la sécurité des réseaux et des systèmes d'information qu'ils utilisent dans le cadre de leurs activités ou de la	

4. Les États membres veillent à ce que les pouvoirs prévus aux paragraphes 1, 2 et 3 ne puissent être exercés que sous réserve de garanties appropriées. Ces garanties font en sorte, en particulier, que les pouvoirs soient exercés de manière objective, transparente et proportionnée et que les droits et les intérêts légitimes des entités critiques concernées, tels que la protection des secrets commerciaux et d'affaires, soient dûment préservés, ce qui comprend le droit d'être entendu, les droits de la défense et le droit à un recours effectif devant une juridiction indépendante. 5. Les États membres veillent à ce que, lorsqu'une autorité compétente en vertu de la présente directive évalue le respect par une entité critique de	des règles de sécurité prévues à l'article L. 1332-6-1. Les contrôles sont effectués par l'autorité nationale de sécurité des systèmes d'information ou par des services de l'Etat désignés par le Premier ministre ou par des prestataires de service qualifiés par ce dernier. Le coût des contrôles est à la charge de l'opérateur.		fourniture de leurs services, les opérateurs d'importance vitale mettent en œuvre les obligations prévues aux articles 14 et 16, et au premier alinéa de l'article 17 de la loi n° XXX relative à la résilience des infrastructures critiques et au renforcement de la cybersécurité. **Article L. 1332-12** Sont habilités à rechercher et constater les infractions et manquements aux prescriptions du présent chapitre, à l'exception de l'article L. 1332-11, ainsi qu'aux dispositions réglementaires prises	

ses obligations en vertu du présent article, ladite autorité compétente en informe les autorités compétentes des États membres concernés en vertu de la directive (UE) 2022/2555 À cette fin, les États membres veillent à ce que les autorités compétentes en vertu de la présente directive puissent demander aux autorités compétentes en vertu de la directive (UE) 2022/2555 d'exercer leurs pouvoirs de supervision et d'exécution à l'égard d'une entité relevant de ladite directive qui a été désignée en tant qu'entité critique en vertu de la présente directive. À cette fin, les États membres veillent à ce que les autorités compétentes en vertu de la présente directive coopèrent et échangent des informations avec les autorités compétentes en vertu de la			pour son application, en vue de la saisine de la commission prévue à l'article L. 1332-15, les agents de l'Etat spécialement désignés et assermentés à cette fin dans des conditions précisées par décret en Conseil d'Etat **Article L. 1332-13 :** Les agents mentionnés à l'article L. 1332-12 ont accès, pour l'exercice de leurs missions, aux locaux des opérateurs d'importance vitale. Ils peuvent pénétrer dans les lieux à usage professionnel ou dans les lieux d'exécution d'une prestation de service.	

directive (UE) 2022/2555.			Ils peuvent 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'Etat et des collectivités territoriales, ainsi que dans les entreprises ou services concédés par l'Etat, les régions, les départements et les communes. Ils peuvent recueillir, sur place ou sur convocation, tout renseignement, toute justification ou tout document nécessaire aux contrôles. A ce titre, ils peuvent exiger la communication de	

			documents de toute nature propres à faciliter l'accomplissement de leur mission. Ils peuvent les obtenir ou en prendre copie, par tout moyen et sur tout support, ou procéder à la saisie de ces documents en quelques mains qu'ils se trouvent. Ils peuvent procéder, sur convocation ou sur place, aux auditions de toute personne susceptible d'apporter des éléments utiles à leurs constatations. Ils en dressent procès-verbal. Les personnes entendues procèdent elles-mêmes à sa lecture, peuvent y faire consigner leurs	

			observations et y apposent leur signature. En cas de refus de signer le procès-verbal, mention en est faite sur celui-ci. Ils sont astreints au secret professionnel pour les faits, actes ou renseignements dont ils ont pu avoir connaissance en raison de leurs fonctions, dans les conditions prévues à l'article 226-13 du code pénal. Le secret professionnel ne peut leur être opposé. Les infractions et les manquements sont constatés par des procès-verbaux, qui font foi	

			jusqu'à preuve contraire. Il est dressé procès-verbal des vérifications et visites menées en application du présent article. **Article L. 1332-14** Il est interdit de faire obstacle à l'exercice des fonctions des agents habilités. L'opérateur contrôlé est tenu de coopérer avec l'autorité administrative. Les agents mentionnés à l'article L. 1332-12 peuvent constater toute action de l'opérateur d'importance vitale de nature à faire obstacle au contrôle.	

			Le fait pour quiconque de faire obstacle aux demandes de l'autorité compétente nécessaires à la recherche des manquements et à la mise en œuvre de ses pouvoirs de contrôle prévus par la présente sous-section, notamment en fournissant des renseignements incomplets ou inexacts, ou en communiquant des pièces incomplètes ou dénaturées, est puni d'une amende administrative prononcée par la commission des sanctions mentionnée à l'article L. 1332-15 dont le montant, proportionné à la gravité du manquement, ne peut	

			excéder 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, le montant le plus élevé étant retenu. Ces dispositions ne s'appliquent pas à l'Etat et à ses établissements publics qui font l'objet d'un contrôle.	
Article 22 **Sanctions** Les États membres déterminent le **régime des sanctions applicables aux violations des dispositions nationales**	**Article L. 1332-7** Est puni d'une amende de 150 000 euros le fait, pour les dirigeants des opérateurs mentionnés à l'article L. 1332-4 et	Mesures de nature législative relative à une procédure de sanction administrative ayant un impact potentiellement conséquent sur les opérateurs à l'issue de contrôles portant sur le	**Article L. 1332-14** Il est interdit de faire obstacle à l'exercice des fonctions des agents habilités. L'opérateur contrôlé est tenu de coopérer avec l'autorité	Dans un constant souci de cohérence et d'harmonisation d'un dispositif de sanction applicable aux opérateurs et ainsi que le prévoit la directive, le Gouvernement a opté pour un mécanisme

adoptées conformément à la présente directive et prennent toutes les mesures nécessaires pour assurer la mise en œuvre de ces sanctions. Ces sanctions doivent être effectives, proportionnées et dissuasives. Les États membres informent la Commission, au plus tard le 17 octobre 2024 du régime ainsi déterminé et des mesures ainsi prises, de même que, sans retard, de toute modification apportée ultérieurement à ce régime ou à ces mesures.	à l'expiration du délai défini par l'arrêté de mise en demeure, d'omettre d'établir un plan de protection ou de réaliser les travaux prévus. Est puni d'une amende de 150 000 euros le fait, pour les mêmes personnes, d'omettre, après une mise en demeure, d'entretenir en bon état les dispositifs de protection antérieurement établis. Est puni d'une amende de 150 000 € le fait, pour les mêmes personnes, de ne pas satisfaire aux obligations prévues aux articles L. 1332-6-	respect de dispositions relevant du législateur en matière de Défense nationale. Un décret en Conseil d'Etat précisera les modalités de mise en œuvre de cette procédure.	administrative. Les agents mentionnés à l'article L. 1332-12 peuvent constater toute action de l'opérateur d'importance vitale de nature à faire obstacle au contrôle. Le fait pour quiconque de faire obstacle aux demandes de l'autorité compétente nécessaires à la recherche des manquements et à la mise en œuvre de ses pouvoirs de contrôle prévus par la présente sous-section, notamment en fournissant des renseignements incomplets ou inexacts, ou en communiquant des pièces incomplètes ou	unique de sanction administrative pouvant être le cas échéant prononcée par une commission placée auprès du Premier ministre qui n'est ni une commission administrative au sens du CRPA, ni une juridiction. Afin de garantir l'effectivité, la proportionnalité et le caractère dissuasif des sanctions, le Gouvernement a souhaité harmoniser les sanctions pécuniaires envisagées avec celles expressément prévues par la directive « NIS 2 » (cf. titre II du projet). Ces dispositions du projet de loi assurent donc la correcte transposition de l'article 22 de la directive. L'exonération de ce

	1 à L. 1332-6-4. Hormis le cas d'un manquement à l'article L. 1332-6-2, cette sanction est précédée d'une mise en demeure. Les personnes morales déclarées responsables, dans les conditions prévues à l'article 121-2 du code pénal, des infractions prévues à la présente section encourent une amende suivant les modalités prévues à l'article 131-38 du même code**.**		dénaturées, est puni d'une amende administrative prononcée par la commission des sanctions mentionnée à l'article L. 1332-15 dont le montant, proportionné à la gravité du manquement, ne peut excéder 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, le montant le plus élevé étant retenu. Ces dispositions ne s'appliquent pas à l'Etat et à ses établissements publics qui font l'objet d'un contrôle.	dispositif de sanctions pour l'Etat et les collectivités territoriales se justifie légalement par l'existence de moyens distincts pour le Gouvernement de contraindre ces opérateurs au respect des dispositions applicables. En outre, l'Etat ne pourrait être condamné à se verser à lui-même une amende administrative dès lors que le produit de ces amendes est versé au Trésor public.

			Article L. 1332-15 Tout manquement aux dispositions du présent chapitre peut donner lieu aux sanctions prévues à l'article L. 1332-17, prononcées par une commission des sanctions instituée à cet effet auprès du Premier ministre. Cette commission est saisie par l'autorité administrative des manquements constatés lors des contrôles effectués en application de l'article L. 1332-13. Cette autorité notifie à l'opérateur concerné les griefs susceptibles d'être	

			retenus à son encontre. La commission des sanctions reçoit les rapports et procès-verbaux des contrôles **Article L. 1332-16** La commission des sanctions mentionnée à l'article L. 1332-15 est composée : 1° D'un membre du Conseil d'Etat, président, désigné par le vice-président du Conseil d'Etat, d'un membre de la Cour de cassation	

			désigné par le premier président de la Cour de cassation, d'un membre de la Cour des comptes désigné par le premier président de la Cour des comptes ; 2° Et de trois personnalités qualifiées nommées par le Premier ministre en raison de leurs compétences dans le domaine de la sécurité des activités d'importance vitale. Un suppléant est désigné dans les mêmes conditions pour les membres mentionnés au 1°.	

			Les membres de la commission des sanctions exercent leurs fonctions en toute impartialité. Dans l'exercice de leurs attributions, ils ne reçoivent ni ne sollicitent d'instruction d'aucune autorité. Le président de la commission désigne un rapporteur parmi ses membres. Celui-ci ne peut recevoir aucune instruction. La commission des sanctions statue par décision motivée.	

			Aucune sanction ne peut être prononcée sans que l'opérateur concerné ou son représentant ait été entendu ou, à défaut, dûment convoqué. La commission peut auditionner toute personne qu'elle juge utile. La commission statue à la majorité des membres présents. En cas de partage égal des voix, celle du président est prépondérante. Le président et les membres de la commission ainsi que leurs suppléants respectifs sont nommés	

			par décret pour un mandat de cinq ans, renouvelable une fois. Ils sont tenus au secret professionnel **Article L. 1332-17** I - En cas de manquement aux obligations découlant de l'application des dispositions du présent chapitre, la commission des sanctions peut prononcer à l'encontre des opérateurs d'importance vitale, à l'exception des administrations de l'Etat et de ses établissements publics administratifs, des collectivités territoriales, de leurs groupements et de leurs	

			établissements publics administratifs, une amende administrative dont le montant, proportionné à la gravité du manquement, ne peut excéder 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, le montant le plus élevé étant retenu. Lorsque la commission des sanctions envisage également de prononcer la sanction prévue au deuxième alinéa de l'article L. 1332-14, le montant cumulé ne peut excéder le montant maximum prévu à	

			l'alinéa précédent. II. - En cas de manquement constaté aux obligations découlant de l'application des dispositions mentionnées aux 1° à 5° de l'article 26 de la loi n° XXXX relative à la résilience des infrastructures critiques et au renforcement de la cybersécurité, la commission des sanctions, dans la composition prévue à l'article 36 de cette loi, peut prononcer les sanctions prévues à l'article 28 et à l'article 37 ter de la même loi.	

			Article L. 1332-18 La commission des sanctions peut ordonner la publication, la diffusion ou l'affichage de la sanction pécuniaire ou d'un extrait de celle-ci, selon les modalités qu'elle précise. Les frais sont supportés par la personne sanctionnée. Les sanctions pécuniaires sont versées au Trésor public et recouvrées comme créances de l'Etat étrangères à l'impôt et au domaine. Les recours formés contre les décisions de la commission des	

			sanctions sont des recours de pleine juridiction. **Article L. 1332-19** Les conditions d'application de la présente sous-section, notamment les règles de fonctionnement de la commission et les modalités de récusation de ses membres, sont définies par décret en Conseil d'Etat.	
Article 23 **Exercice de la délégation** 1. Le pouvoir d'adopter des actes délégués conféré à la	Sans objet	Sans objet	Sans objet	Ces dispositions relatives aux prérogatives de la Commission n'impliquent aucune mesure de transposition

Commission est soumis aux conditions fixées au présent article. 2. Le pouvoir d'adopter des actes délégués visé à l'article 5, paragraphe 1, est conféré à la Commission pour une période de cinq ans à compter du 16 janvier 2023. 3. La délégation de pouvoir visée à l'article 5, paragraphe 1, peut être révoquée à tout moment par le Parlement européen ou le Conseil. La décision de révocation met fin à la délégation de pouvoir qui y est précisée. La révocation prend effet le jour suivant celui de la publication de ladite décision au Journal officiel de l'Union européenne ou à une date ultérieure qui est précisée dans ladite décision. Elle ne porte pas atteinte à la validité des actes				

délégués déjà en vigueur. 4. Avant l'adoption d'un acte délégué, la Commission consulte les experts désignés par chaque État membre, conformément aux principes définis dans l'accord interinstitutionnel du 13 avril 2016 « Mieux légiférer ». 5. Aussitôt qu'elle adopte un acte délégué, la Commission le notifie au Parlement européen et au Conseil simultanément. 6. Un acte délégué adopté en vertu de l'article 5, paragraphe 1, n'entre en vigueur que si le Parlement européen ou le Conseil n'a pas exprimé d'objections dans un délai de deux mois à compter de la notification de cet acte au Parlement européen et au Conseil ou si, avant l'expiration de ce délai, le Parlement européen et le Conseil ont tous				

deux informé la Commission de leur intention de ne pas exprimer d'objections. Ce délai est prolongé de deux mois à l'initiative du Parlement européen ou du Conseil. **Article 24** **Comité** 1. La Commission est assistée par un comité. Ledit comité est un comité au sens du règlement (UE) no 182/2011. 2. Lorsqu'il est fait référence au présent paragraphe, l'article 5 du règlement (UE) no 182/2011 s'applique. **Article 25** **Rapports et réexamen** Au plus tard le 17 juillet 2027, la				

Commission présente au Parlement européen et au Conseil un rapport évaluant la mesure dans laquelle chaque État membre a pris les dispositions nécessaires pour se conformer à la présente directive. La Commission réexamine périodiquement le fonctionnement de la présente directive et fait rapport au Parlement européen et au Conseil. Ce rapport évalue en particulier la valeur ajoutée de la présente directive, son impact en vue de garantir la résilience des entités critiques et détermine si l'annexe de la présente directive devrait être modifiée. La Commission présente le premier rapport de ce type au plus tard le 17 juin 2029. Aux fins de l'établissement des rapports au titre du présent article, la				

Commission tient compte des documents pertinents du groupe sur la résilience des entités critiques.				
Article 26 **Transposition** 1. Les États membres adoptent et publient, au plus tard le 17 octobre 2024, les dispositions nécessaires pour se conformer à la présente directive. Ils en informent immédiatement la Commission. Ils appliquent ces dispositions à partir du 18 octobre 2024. 2. Lorsque les États membres adoptent les dispositions visées au paragraphe 1, celles-ci contiennent une référence à la présente directive ou sont	Sans objet	Mesures de nature législatives concernant des dispositions transitoires portant sur des obligations légales	**Article 4 du projet de loi** **Dispositions transitoires** Les opérateurs d'importance vitale désignés avant la date d'entrée en vigueur des dispositions du titre I^{er} de la présente loi sont regardés comme désignés en application du I de l'article L. 1332-2 du code de la défense dans sa rédaction résultant du chapitre I^{er} de la présente loi à la date de son entrée en vigueur.	Les mesures transitoires que le Gouvernement propose concernent uniquement les opérateurs désignés au titre de la législation actuelle pour lesquels une continuité s'impose. En effet, les opérateurs actuels n'auront pas à être désignés au titre de la législation nouvelle et ils bénéficieront des mêmes garanties accordées aux futurs opérateurs désignés, notamment s'agissant des délais accordés pour établir les documents de planification.

accompagnées d'une telle référence lors de leur publication officielle. Les modalités de cette référence sont arrêtées par les États membres.			Ces opérateurs restent soumis aux obligations qui leurs sont applicables avant la date d'entrée en vigueur de la présente loi jusqu'à l'accomplissement des obligations prévues aux articles L. 1332-2 à L. 1332-5 et à l'article L. 1332-11 du code de la défense dans leur rédaction résultant de la présente loi.	Pour autant, il est apparu indispensable de prévoir les dispositions permettant de s'assurer que ces anciens opérateurs désignés continuent à mettre en œuvre leurs obligations en cours.
Article 27 **Abrogation de la directive 2008/114/CE** La directive 2008/114/CE est abrogée avec effet au 18 octobre 2024. Les références faites à la	Sans objet	Sans objet	Sans objet	Sans objet

directive abrogée s'entendent comme faites à la présente directive. **Article 28** **Entrée en vigueur** La présente directive entre en vigueur le vingtième jour suivant celui de sa publication au Journal officiel de l'Union européenne. **Article 29** **Destinataires** Les États membres sont destinataires de la présente directive.				

ANNEXE II – TABLEAU DE TRANSPOSITION DE LA DIRECTIVE (UE) 2022/2555 (DITE DIRECTIVE NIS2) DU PARLEMENT EUROPEEN ET DU CONSEIL DU 14 DECEMBRE 2022 CONCERNANT DES MESURES DESTINEES A ASSURER UN NIVEAU ELEVE COMMUN DE CYBERSECURITE DANS L'ENSEMBLE DE L'UNION, MODIFIANT LE REGLEMENT (UE) N° 910/2014 ET LA DIRECTIVE (UE) 2018/1972 ET ABROGEANT LA DIRECTIVE (UE) 2016/1148

Mesure de transposition prévue dans le projet de loi	**Disposition de la directive**	**Normes à adopter en vue de la transposition**	**Observations générales et relatives à l'impact de la disposition de la directive**
N/A	Art. 1er, 1. La présente directive établit des mesures qui ont pour but d'obtenir un niveau commun élevé de cybersécurité dans l'ensemble de l'Union, afin d'améliorer le fonctionnement du marché intérieur.		
N/A	Art. 1er, 2. À cette fin, la présente directive fixe: a) des obligations qui imposent aux États membres d'adopter des stratégies nationales		

	en matière de cybersécurité, de désigner ou de mettre en place des autorités compétentes, des autorités chargées de la gestion des cybercrises, des points de contact uniques en matière de cybersécurité (ci-après dénommés «points de contact uniques») et des centres de réponse aux incidents de sécurité informatique (CSIRT); b) des mesures de gestion des risques en matière de cybersécurité et des obligations d'information pour les entités d'un type visé à l'annexe I ou II, ainsi que pour les entités recensées en tant qu'entités critiques en vertu de la directive (UE) 2022/ 2557; c) des règles et des obligations pour le partage d'informations en matière de cybersécurité; d) les obligations des États membres en matière de supervision et d'exécution.		
Art. 8, 1° et 2° Sont des entités essentielles : 1° Les entreprises appartenant à un des secteurs d'activité hautement critiques qui emploient au moins 250 personnes ou dont le chiffre d'affaires annuel excède 50 millions d'euros et dont le total du bilan annuel excède 43 millions d'euros ; 2° Les établissements publics à caractère industriel et commercial, à l'exception du Commissariat à l'énergie	<u>Art. 2, 1.</u> La présente directive s'applique aux entités publiques ou privées d'un type visé à l'annexe I ou II qui constituent des entreprises moyennes en vertu de l'article 2 de l'annexe de la recommandation 2003/361/CE, ou qui dépassent les plafonds prévus au paragraphe 1 dudit article, et qui fournissent leurs services ou exercent leurs	Norme de niveau législatif, qui sera à décliner par un décret.	Cf. Fiche d'impact « Périmètre de compétence de l'ANSSI et exigences de sécurité ».

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, 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 par le 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 ; Art. 9, 1° et 8° Sont des entités importantes : 1° Les entreprises appartenant à un des secteurs d'activité hautement critiques ou critiques qui ne sont pas des entités essentielles et qui emploient au moins 50 personnes ou dont le chiffre d'affaires et le total du bilan annuel excèdent chacun 10 millions d'euros ; […] 8° Les établissements publics à caractère industriel et commercial et 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.	activités au sein de l'Union. L'article 3, paragraphe 4, de l'annexe de ladite recommandation ne s'applique pas aux fins de la présente directive.		

2221-4 du code général des collectivités territoriales, relevant des secteurs d'activité hautement critiques ou critiques, qui emploient au moins 50 personnes ou dont le produit d'exploitation et le total du bilan annuel excèdent chacun 10 millions d'euros et qui ne sont pas entités essentielles. Le critère d'emploi est calculé selon les modalités prévues par le 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.			
Art. 8, 3° à 6° Sont des entités essentielles : 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 ; 4° Les prestataires de service de confiance qualifiés ; 5° Les offices d'enregistrement ; 6° Les fournisseurs de services de système de noms de domaine ; Art. 9, 2° Sont des entités importantes : 2° Les opérateurs de communications électroniques	<u>Art. 2, 2.</u> La présente directive s'applique également aux entités d'un type visé à l'annexe I ou II, quelle que soit leur taille, dans les cas suivants : a) Les services sont fournis par : i. Des fournisseurs de réseaux de communications électroniques publics ou de services de communications électroniques accessibles au public ; ii. Des prestataires de services de confiance ; iii. Des registres des noms de domaine de premier niveau et des fournisseurs de services de système de noms de domaine ;	Norme de niveau législatif, qui sera à décliner par un décret.	Cf. Fiche d'impact « Périmètre de compétence de l'ANSSI et exigences de sécurité ». Prise en compte de la définition dans le droit national de la notion de fournisseurs de réseaux de communications électroniques publics ou de services de communications électroniques accessibles au public

qui ne sont pas des entités essentielles ;			
Art. 10, 1° Outre les entités mentionnées aux articles 8 et 9, 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 l'un des critères suivants : 1° L'entité est le seul prestataire sur le territoire national d'un service qui est essentiel au maintien du fonctionnement de la société et d'activités économiques critiques ;	b) l'entité est, dans un État membre, le seul prestataire d'un service qui est essentiel au maintien d'activités sociétales ou économiques critiques;	Norme de niveau législatif, qui sera à décliner par un décret.	Cf. Fiche d'impact « Périmètre de compétence de l'ANSSI et exigences de sécurité ».
Art. 10, 2° Outre les entités mentionnées aux articles 8 et 9, 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 l'un des critères suivants : 2° Une perturbation du service fourni par l'entité pourrait avoir un impact important sur la sécurité	c) une perturbation du service fourni par l'entité pourrait avoir un impact important sur la sécurité publique, la sûreté publique ou la santé publique;	Norme de niveau législatif, qui sera à décliner par un décret.	Cf. Fiche d'impact « Périmètre de compétence de l'ANSSI et exigences de sécurité ».

publique, la sûreté publique ou la santé publique ;			
Art. 10, 3° Outre les entités mentionnées aux articles 8 et 9, 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 l'un des critères suivants : 3° 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) 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 ;	Norme de niveau législatif, qui sera à décliner par un décret.	Cf. Fiche d'impact « Périmètre de compétence de l'ANSSI et exigences de sécurité ».
Art. 10, 4° Outre les entités mentionnées aux articles 8 et 9, 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 l'un des critères suivants : 4° Une perturbation du service fourni par l'entité pourrait induire un risque systémique important, en	e) 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; L 333/108 FR Journal officiel de l'Union européenne 27.12.2022	Norme de niveau législatif, qui sera à décliner par un décret.	Cf. Fiche d'impact « Périmètre de compétence de l'ANSSI et exigences de sécurité ».

particulier pour les secteurs où cette perturbation pourrait avoir un impact transfrontière ;			
Art. 8, 2° Sont des entités essentielles : 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, 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 par le 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 ; Art. 8, 7°, a) à h) Sont des entités essentielles : 7° Les administrations suivantes : a) Les administrations de l'Etat et leurs établissements publics administratifs, à l'exception des administrations de l'Etat qui	f) l'entité est une entité de l'administration publique: i. des pouvoirs publics centraux tels qu'ils sont définis par un État membre conformément au droit national; ou ii. au niveau régional, tel qu'il est défini par un État membre conformément au droit national, qui, à la suite d'une évaluation basée sur les risques, fournit des services dont la perturbation pourrait avoir un impact important sur des activités sociétales ou économiques critiques.	Norme de niveau législatif, qui sera à décliner par voie règlementaire.	Cf. Fiche d'impact « Périmètre de compétence de l'ANSSI et exigences de sécurité ».

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 établissements publics administratifs 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'Etat 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'Etat ; b) Les régions, les départements, les communes d'une population supérieure à 30 000 habitants, leurs établissements publics administratifs dont les activités s'inscrivent dans un des secteurs d'activité hautement critiques ou critiques ; c) Les centres de gestion mentionnés à l'article L. 452-1 du code général de la fonction publique ; d) Les services départementaux d'incendie et de secours mentionnés à l'article L. 1424-1 du code général des collectivités territoriales ;			

e) Les communautés urbaines, les communautés d'agglomération et les métropoles, leurs établissements publics administratifs dont les activités s'inscrivent dans un des secteurs d'activité hautement critiques ou critiques ; f) Les syndicats mentionnés aux articles L. 5212-1, L. 5711-1 et L. 5721-2 du code général des collectivités territoriales dont les activités s'inscrivent dans un des secteurs d'activité hautement critiques ou critiques et dont la population est supérieure à 30 000 habitants ; g) Les institutions et organismes interdépartementaux mentionnés à l'article L. 5421-1 du code général des collectivités territoriales dont les activités s'inscrivent dans un des secteurs d'activité hautement critiques ou critiques ; h) Et 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'Etat ; Art. 9, 4°, 6°, 7° et 8° Sont des entités importantes : 4° Les communautés de communes et leurs établissements publics administratifs dont les activités s'inscrivent dans un des secteurs d'activité hautement critiques ou critiques ; 5° Les établissements d'enseignement menant des activités de recherche qui ne sont pas des entités essentielles. Le Premier ministre désigne par arrêté les établissements qui, compte tenu du faible impact économique et social de leur activité, ne sont pas soumis à la présente loi, dans les conditions précisées par décret en Conseil d'Etat ; 6° Les établissement publics administratifs de l'Etat expressément désignés en tant qu'entités importantes par arrêté du Premier ministre dans des conditions fixées par décret en Conseil d'Etat ; 7° 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, expressément désignés en tant qu'entités importantes par arrêté du Premier ministre dans les conditions			

précisées par décret en Conseil d'Etat ; 8° Les établissements publics à caractère industriel et commercial et 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 des secteurs d'activité hautement critiques ou critiques, qui emploient au moins 50 personnes ou dont le produit d'exploitation et le total du bilan annuel excèdent chacun 10 millions d'euros et qui ne sont pas entités essentielles. Le critère d'emploi est calculé selon les modalités prévues par le 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.			
Art. 8, 8° Sont des entités essentielles : 8° Les opérateurs d'importance vitale en tant qu'ils exercent une activité qualifiée de service essentiel en application du deuxième alinéa du 1° du I de l'article L. 1332-2 du code de la défense ;	Art. 2, 3. La présente directive s'applique aux entités recensées en tant qu'entités critiques en vertu de la directive (UE) 2022/ 2557, quelle que soit leur taille.		Cf. Fiche d'impact « Périmètre de compétence de l'ANSSI et exigences de sécurité ». La rédaction s'appuie sur la transposition faite dans la loi proposée de la directive (UE) 2022/2557

Art. 8, 5°, 6° Sont des entités essentielles : 5° Les offices d'enregistrement ; 6° Les fournisseurs de services de système de noms de domaine ; Art. 11, 3° 3° S'agissant des fournisseurs de services de système de noms de domaine, des offices d'enregistrement, des fournisseurs de services d'informatique en nuage, des fournisseurs de services de centres de données, des fournisseurs de réseaux de diffusion de contenu, des fournisseurs de services gérés, des fournisseurs de services de sécurité gérés, ainsi que des fournisseurs de places de marché en ligne, de moteurs de recherche en ligne ou de plateformes de services de réseaux sociaux : a) Ils ont leur établissement principal sur le territoire national ; b) Ou, s'ils sont établis hors de l'Union européenne mais offrent leurs services sur le territoire national, ils ont désigné un représentant établi sur le territoire national. Art. 18 Les offices d'enregistrement et les bureaux	Art. 2, 4. La présente directive s'applique aux entités fournissant des services d'enregistrement de noms de domaine, quelle que soit leur taille.		Cf. Fiche d'impact « Périmètre de compétence de l'ANSSI et exigences de sécurité ».

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 sont soumis aux dispositions de la présente section.			
Art. 8, 7°, b) à h) Sont des entités essentielles : 7° Les administrations suivantes : b) Les régions, les départements, les communes d'une population supérieure à 30 000 habitants, leurs établissements publics administratifs dont les activités s'inscrivent dans un des secteurs d'activité hautement critiques ou critiques ; c) Les centres de gestion mentionnés à l'article L. 452-1 du code général de la fonction publique ; d) Les services départementaux d'incendie et de secours mentionnés à l'article L. 1424-1 du code général des collectivités territoriales ; e) Les communautés urbaines, les communautés d'agglomération et les métropoles, leurs établissements publics administratifs dont les activités s'inscrivent dans un des secteurs d'activité hautement critiques ou critiques ; f) Les syndicats mentionnés aux articles L. 5212-1, L. 5711-1 et L. 5721-2 du code général des collectivités territoriales dont les activités s'inscrivent dans un des secteurs d'activité hautement critiques ou critiques et dont la	<u>Art. 2, 5.</u> Les États membres peuvent prévoir que la présente directive s'applique: a) aux entités de l'administration publique au niveau local; b) aux établissements d'enseignement, en particulier lorsqu'ils mènent des activités de recherche critiques	Norme de niveau législatif, qui sera à décliner par voie règlementaire.	Cf. Fiche d'impact « Périmètre de compétence de l'ANSSI et exigences de sécurité ».

population est supérieure à 30 000 habitants ; g) Les institutions et organismes interdépartementaux mentionnés à l'article L. 5421-1 du code général des collectivités territoriales dont les activités s'inscrivent dans un des secteurs d'activité hautement critiques ou critiques ; h) Et 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'Etat ; Art. 8, 10° Sont des entités essentielles : 10° Les établissements d'enseignement menant des activités de recherche désignés par arrêté du Premier ministre dans des conditions précisées par décret en Conseil d'Etat, qui remplissent l'un des critères mentionnés à l'article 10.			

Art. 9, 4° et 5° Sont des entités importantes : 4° Les communautés de communes et leurs établissements publics administratifs dont les activités s'inscrivent dans un des secteurs d'activité hautement critiques ou critiques ; 5° Les établissements d'enseignement menant des activités de recherche qui ne sont pas des entités essentielles. Le Premier ministre désigne par arrêté les établissements qui, compte tenu du faible impact économique et social de leur activité, ne sont pas soumis à la présente loi, dans les conditions précisées par décret en Conseil d'Etat ;			
N/A	Art. 2, 6. La présente directive est sans préjudice de la responsabilité des États membres en matière de sauvegarde de la sécurité nationale et de leur pouvoir de garantir d'autres fonctions essentielles de l'État, notamment celles qui ont pour objet d'assurer l'intégrité territoriale de l'État et de maintenir l'ordre public		
Art. 8, 7°, a) Sont des entités essentielles :	Art. 2, 7. La présente directive ne s'applique pas aux entités de l'administration publique qui exercent leurs activités dans les domaines de la sécurité nationale,	Norme de niveau législatif, qui sera à	Cf. Fiche d'impact « Périmètre de compétence de l'ANSSI et exigences de

7° Les administrations suivantes : a) Les administrations de l'Etat et leurs établissements publics administratifs, à l'exception des administrations de l'Etat 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 établissements publics administratifs 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'Etat 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'Etat ;	de la sécurité publique, de la défense ou de l'application de la loi, y compris la prévention et la détection des infractions pénales, ainsi que les enquêtes et les poursuites en la matière.	décliner par voie règlementaire.	sécurité ».
N/A	<u>Art. 2, 8.</u> Les États membres peuvent exempter des entités spécifiques qui exercent des activités dans les domaines de la sécurité nationale, de la sécurité publique, de la défense ou de l'application de la loi, y compris la prévention et la détection des infractions pénales, ainsi que les enquêtes et les		La France a choisi de ne pas saisir cette possibilité.

	poursuites en la matière, ou qui fournissent des services exclusivement aux entités de l'administration publique visées au paragraphe 7 du présent article, des obligations prévues à l'article 21 ou 23 en ce qui concerne ces activités ou services. Dans de tels cas, les mesures de supervision et d'exécution visées au chapitre VII ne s'appliquent pas à ces activités ou services spécifiques. Lorsque les entités exercent des activités ou fournissent des services exclusivement du type visé au présent paragraphe, les États membres peuvent également décider d'exempter ces entités des obligations prévues aux articles 3 et 27.		
Art. 8, 4° Sont des entités essentielles : 4° Les prestataires de service de confiance qualifiés ; Art. 9, 3° Sont des entités importantes : 3° Les prestataires de service de confiance qui ne sont pas des entités essentielles ;	Art. 2, 9. Les paragraphes 7 et 8 ne s'appliquent pas lorsqu'une entité agit en tant que prestataire de services de confiance.		Cf. Fiche d'impact « Périmètre de compétence de l'ANSSI et exigences de sécurité ».
N/A	Art. 2, 10. La présente directive ne s'applique pas aux entités que les États membres ont exclues du champ		

	d'application du règlement (UE) 2022/2554 conformément à l'article 2, paragraphe 4, dudit règlement.		
N/A	Art. 2, 11. Les obligations énoncées dans la présente 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.		
N/A	Art. 2, 12. La présente directive est sans préjudice du règlement (UE) 2016/679, de la directive 2002/58/CE, des directives 2011/93/UE ([27]) et 2013/40/UE ([28]) du Parlement européen et du Conseil et de la directive (UE) 2022/2557.		
N/A	Art. 2, 13. 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 et d'autres autorités		

	concernées conformément à la présente 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.		
N/A	Art. 2, 14. Les entités, les autorités compétentes, les points de contact uniques et les CSIRT traitent les données à caractère personnel dans la mesure nécessaire aux fins de la présente directive et conformément au règlement (UE) 2016/679; ce traitement est fondé en particulier sur l'article 6 dudit règlement. Le traitement des données à caractère personnel en vertu de la présente directive par les fournisseurs de réseaux de communications électroniques publics ou les fournisseurs de services de communications électroniques accessibles au public est effectué conformément au droit de l'Union en matière de protection des données et au droit de l'Union en matière de protection de la vie privée, en particulier la directive 2002/58/CE.		
Art. 8, 1°	Art. 3, 1.	Norme de niveau	Cf. Fiche d'impact « Périmètre de

Sont des entités essentielles : 1° Les entreprises appartenant à un des secteurs d'activité hautement critiques qui emploient au moins 250 personnes ou dont le chiffre d'affaires annuel excède 50 millions d'euros et dont le total du bilan annuel excède 43 millions d'euros ;	Aux fins de la présente directive, les entités suivantes sont considérées comme étant des entités essentielles : 1) les entités d'un type visé à l'annexe I qui dépassent les plafonds applicables aux moyennes entreprises prévus à l'article 2, paragraphe 1, de l'annexe de la recommandation 2003/361/CE;	législatif, qui sera à décliner par voie règlementaire.	compétence de l'ANSSI et exigences de sécurité ».
Art. 8, 4° à 6° Sont des entités essentielles : 4° Les prestataires de service de confiance qualifiés ; 5° Les offices d'enregistrement ; 6° Les fournisseurs de services de système de noms de domaine ;	<u>Art. 3, 1.</u> Aux fins de la présente directive, les entités suivantes sont considérées comme étant des entités essentielles : 2) les prestataires de services de confiance qualifiés et les registres de noms de domaine de premier niveau ainsi que les fournisseurs de services DNS, quelle que soit leur taille;		Cf. Fiche d'impact « Périmètre de compétence de l'ANSSI et exigences de sécurité ».
Art. 8, 3° Sont des entités essentielles : 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 ;	<u>Art. 3, 1.</u> Aux fins de la présente directive, les entités suivantes sont considérées comme étant des entités essentielles: 3) les fournisseurs de réseaux publics de communications électroniques publics ou de services de communications électroniques accessibles au public qui	Norme de niveau législatif, qui sera à décliner par voie règlementaire.	Cf. Fiche d'impact « Périmètre de compétence de l'ANSSI et exigences de sécurité ».

	constituent des moyennes entreprises en vertu de l'article 2 de l'annexe de la recommandation 2003/361/CE ;		
Art. 8, 7°, a) Sont des entités essentielles : 7° Les administrations suivantes : a) Les administrations de l'Etat et leurs établissements publics administratifs, à l'exception des administrations de l'Etat 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 établissements publics administratifs 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'Etat 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'Etat ;	Art. 3, 1. Aux fins de la présente directive, les entités suivantes sont considérées comme étant des entités essentielles: 4) les entités de l'administration publique visées à l'article 2, paragraphe 2, point f) i);	Norme de niveau législatif, qui sera à décliner par voie règlementaire.	Cf. Fiche d'impact « Périmètre de compétence de l'ANSSI et exigences de sécurité ».
Art. 10	Art. 3, 1.	Norme de niveau	Cf. Fiche d'impact « Périmètre de

Outre les entités mentionnées aux articles 8 et 9, 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 l'un des critères suivants : 1° L'entité est le seul prestataire sur le territoire national d'un service qui est essentiel au maintien du fonctionnement de la société et d'activités économiques critiques ; 2° Une perturbation du service fourni par l'entité pourrait avoir un impact important sur la sécurité publique, la sûreté publique ou la santé publique ; 3° 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 ; 4° L'entité est critique en raison de son importance spécifique au niveau national ou local pour le secteur ou le type de service concerné, ou pour d'autres secteurs interdépendants sur le territoire national.	Aux fins de la présente directive, les entités suivantes sont considérées comme étant des entités essentielles : 5) toute autre entité d'un type visé à l'annexe I ou II qui est identifiée par un État membre en tant qu'entité essentielle en vertu de l'article 2, paragraphe 2, points b) à e);	législatif, qui sera à décliner par un décret.	compétence de l'ANSSI et exigences de sécurité ».
Art. 8, 8° Sont des entités essentielles :	<u>Art. 3, 1.</u> Aux fins de la présente directive, les entités		Cf. Fiche d'impact « Périmètre de compétence de l'ANSSI

8° Les opérateurs d'importance vitale en tant qu'ils exercent une activité qualifiée de service essentiel en application du deuxième alinéa du 1° du I de l'article L. 1332-2 du code de la défense ;	suivantes sont considérées comme étant des entités essentielles : 6) les entités recensées en tant qu'entités critiques en vertu de la directive (UE) 2022/2557, visées à l'article 2, paragraphe 3, de la présente directive;		et exigences de sécurité ».
Art. 8, 9° Sont des entités essentielles : 9° Les opérateurs de services essentiels désignés en application des dispositions 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 ;	Art. 3, 1. Aux fins de la présente directive, les entités suivantes sont considérées comme étant des entités essentielles : 7) si l'État membre en dispose ainsi, les entités que cet État membre a identifiées avant le 16 janvier 2023 comme des opérateurs de services essentiels conformément à la directive (UE) 2016/1148 ou au droit national.		Cf. Fiche d'impact « Périmètre de compétence de l'ANSSI et exigences de sécurité ».
Art. 9, 1° Sont des entités importantes : 1° Les entreprises appartenant à un des secteurs d'activité hautement critiques ou critiques qui ne sont pas des entités essentielles et qui emploient au moins 50 personnes ou dont le chiffre d'affaires et le total du bilan annuel excèdent chacun 10 millions d'euros ; Art. 10	Art. 3, 2. Aux fins de la présente directive, les entités d'un type visé à l'annexe I ou II qui ne constituent pas des entités essentielles en vertu du paragraphe 1 du présent article sont considérées comme des entités importantes. Celles-ci incluent les entités identifiées par un État membre en tant qu'entités importantes en vertu de l'article 2, paragraphe 2, points b) à e).	Norme de niveau législatif, qui sera à décliner par voie règlementaire.	Cf. Fiche d'impact « Périmètre de compétence de l'ANSSI et exigences de sécurité ».

Outre les entités mentionnées aux articles 8 et 9, 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 l'un des critères suivants : 1° L'entité est le seul prestataire sur le territoire national d'un service qui est essentiel au maintien du fonctionnement de la société et d'activités économiques critiques ; 2° Une perturbation du service fourni par l'entité pourrait avoir un impact important sur la sécurité publique, la sûreté publique ou la santé publique ; 3° 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 ; 4° L'entité est critique en raison de son importance spécifique au niveau national ou local pour le secteur ou le type de service concerné, ou pour d'autres secteurs interdépendants sur le territoire national.			
Art. 12 L'autorité nationale de sécurité des systèmes d'information établit et met à jour la liste des entités	Art. 3, 3. Au plus tard le 17 avril 2025, les États membres	Norme de niveau législatif, qui	Cf. Fiche d'impact « Périmètre de compétence de l'ANSSI

essentielles, des entités importantes et des bureaux d'enregistrement sur la base des informations que ces entités et bureaux d'enregistrement lui communiquent. Les informations à transmettre, leurs modalités de communication et les délais dans lesquels les modifications doivent être transmises sont définis par décret en Conseil d'Etat.	établissent une liste des entités essentielles et importantes ainsi que des entités fournissant des services d'enregistrement de noms de domaine. Les États membres réexaminent cette liste et, le cas échéant, la mettent à jour régulièrement et au moins tous les deux ans par la suite.	sera à décliner par un décret.	et exigences de sécurité ».
Art. 12 L'autorité nationale de sécurité des systèmes d'information établit et met à jour la liste des entités essentielles, des entités importantes et des bureaux d'enregistrement sur la base des informations que ces entités et bureaux d'enregistrement lui communiquent. Les informations à transmettre, leurs modalités de communication et les délais dans lesquels les modifications doivent être transmises sont définis par décret en Conseil d'Etat.	<u>Art. 3, 4.</u> Aux fins de l'établissement de la liste visée au paragraphe 3, les États membres exigent des entités visées audit paragraphe qu'elles communiquent aux autorités compétentes au moins les informations suivantes: a) le nom de l'entité; b) l'adresse et les coordonnées actualisées, y compris les adresses électroniques, les plages d'IP et les numéros de téléphone; c) le cas échéant, le secteur et le sous-secteur concernés visés à l'annexe I ou II; et d) le cas échéant, une liste des États membres dans lesquels elles fournissent des services relevant du champ d'application de la présente directive. Les entités visées au paragraphe 3 notifient sans tarder toute modification des informations qu'elles	Norme de niveau législatif, qui sera à décliner par un décret.	Cf. Fiche d'impact « Périmètre de compétence de l'ANSSI et exigences de sécurité ».

	ont communiquées conformément au premier alinéa du présent paragraphe et, en tout état de cause, dans un délai de deux semaines à compter de la date de la modification. La Commission, avec l'aide de l'Agence de l'Union européenne pour la cybersécurité (ENISA), fournit sans retard injustifié des lignes directrices et des modèles concernant les obligations prévues au présent paragraphe. Les États membres peuvent mettre en place des mécanismes nationaux permettant aux entités de s'enregistrer elles-mêmes.		
N/A	<u>Art. 3, 5.</u> Au plus tard le 17 avril 2025, puis tous les deux ans par la suite, les autorités compétentes notifient: a) à la Commission et au groupe de coopération le nombre des entités essentielles et importantes identifiées conformément au paragraphe 3 pour chaque secteur et sous-secteur visé à l'annexe I ou II; et b) à la Commission les informations pertinentes sur le nombre d'entités essentielles et importantes identifiées en vertu de l'article 2, paragraphe 2, points b) à e), le secteur et le sous-secteur visés à l'annexe I ou II auxquels elles		

	appartiennent, le type de service qu'elles fournissent et la disposition, parmi celles figurant à l'article 2, paragraphe 2, points b) à e), en vertu de laquelle elles ont été identifiées.		
N/A	<u>Art. 3, 6.</u> Jusqu'au 17 avril 2025 et à la demande de la Commission, les États membres peuvent notifier à la Commission le nom des entités essentielles et importantes visées au paragraphe 5, point b).		
Art. 13 Les dispositions pertinentes de la présente loi, y compris celles relatives à la supervision, ne sont pas applicables aux entités essentielles et importantes qui sont soumises, en application d'un acte juridique de l'Union européenne, à des exigences sectorielles de sécurité et de notification d'incidents ayant un effet au moins équivalent aux obligations résultant des articles 14 et 17. Pour être équivalentes, les exigences de notification des incidents doivent également prévoir un accès immédiat aux notifications d'incidents par l'autorité nationale de sécurité des systèmes d'information.	<u>Art. 4, 1.</u> Lorsque des actes juridiques sectoriels de l'Union imposent à des entités essentielles ou importantes d'adopter des mesures de gestion des risques en matière de cybersécurité ou de notifier des incidents importants, et lorsque ces exigences ont un effet au moins équivalent à celui des obligations prévues par la présente directive, les dispositions pertinentes de la présente directive, y compris celles relatives à la supervision et à l'exécution prévues au chapitre VII, ne sont pas applicables auxdites entités. Lorsque des actes juridiques sectoriels de l'Union ne couvrent pas toutes les entités d'un secteur spécifique relevant du champ d'application de la présente directive, les dispositions pertinentes de la présente directive continuent de s'appliquer aux entités non couvertes		Cf. Fiche d'impact « Périmètre de compétence de l'ANSSI et exigences de sécurité ».

	par ces actes juridiques sectoriels de l'Union.		
Art. 13 Les dispositions pertinentes de la présente loi, y compris celles relatives à la supervision, ne sont pas applicables aux entités essentielles et importantes qui sont soumises, en application d'un acte juridique de l'Union européenne, à des exigences sectorielles de sécurité et de notification d'incidents ayant un effet au moins équivalent aux obligations résultant des articles 14 et 17. Pour être équivalentes, les exigences de notification des incidents doivent également prévoir un accès immédiat aux notifications d'incidents par l'autorité nationale de sécurité des systèmes d'information.	<u>Art. 4, 2.</u> Les exigences visées au paragraphe 1 du présent article sont considérées comme ayant un effet équivalent aux obligations prévues par la présente directive lorsque: a) les mesures de gestion des risques en matière de cybersécurité ont un effet au moins équivalent à celui des mesures prévues à l'article 21, paragraphes 1 et 2; ou b) l'acte juridique sectoriel de l'Union prévoit un accès immédiat, s'il y a lieu, automatique et direct, aux notifications d'incidents par les CSIRT, les autorités compétentes ou les points de contact uniques en vertu de la présente directive, et lorsque les exigences relatives à la notification des incidents importants sont au moins équivalentes à celles prévues à l'article 23, paragraphes 1 à 6, de la présente directive.		Cf. Fiche d'impact « Périmètre de compétence de l'ANSSI et exigences de sécurité ».
N/A	<u>Art. 4, 3.</u> Au plus tard le 17 juillet 2023, la Commission fournit des lignes directrices clarifiant l'application des paragraphes 1 et 2. La Commission réexamine ces lignes directrices à intervalles réguliers. Lors de la préparation de ces lignes directrices, la		

	Commission tient compte de toutes les observations du groupe de coopération et de l'ENISA.		
N/A	Art. 5 La présente directive ne fait pas obstacle à l'adoption ou au maintien par les États membres de dispositions assurant un niveau plus élevé de cybersécurité, à condition que ces dispositions soient compatibles avec les obligations des États membres prévues par le droit de l'Union.		
Art. 6, 7° 7° Système d'information : l'ensemble des infrastructures et services logiciels informatiques permettant de collecter, traiter, transmettre et stocker sous forme numérique des données.	Art. 6, 1. Aux fins de la présente directive, on entend par: « réseau et système d'information » : a) un réseau de communications électroniques au sens de l'article 2, point 1), de la directive (UE) 2018/1972; b) tout dispositif ou tout ensemble de dispositifs interconnectés ou apparentés, dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement automatisé de données numériques; ou c) les données numériques stockées, traitées, récupérées ou transmises par les		Cf. Fiche d'impact « Définitions ». Cette définition a été adaptée dans le droit national

	éléments visés aux points a) et b) en vue de leur fonctionnement, utilisation, protection et maintenance;		
N/A	Art. 6, 2. « sécurité des réseaux et des systèmes d'information » : la capacité des réseaux et des systèmes d'information de résister, à un niveau de confiance donné, à tout événement susceptible de compromettre la disponibilité, l'authenticité, l'intégrité ou la confidentialité de données stockées, transmises ou faisant l'objet d'un traitement, ou des services que ces réseaux et systèmes d'information offrent ou rendent accessibles;		
N/A	Art. 6, 3. « cybersécurité » : la cybersécurité au sens de l'article 2, point 1), du règlement (UE) 2019/881;		
N/A	Art. 6, 4. «stratégie nationale en matière de cybersécurité»: le cadre cohérent d'un État membre fournissant des objectifs et des priorités stratégiques dans le domaine de la cybersécurité et de la gouvernance en vue de les réaliser dans cet État membre;		

N/A	Art. 6, 5. «incident évité»: un événement qui aurait pu compromettre la disponibilité, l'authenticité, l'intégrité ou la confidentialité des données stockées, transmises ou faisant l'objet d'un traitement, ou des services que les réseaux et systèmes d'information offrent ou rendent accessibles, mais dont la réalisation a pu être empêchée ou ne s'est pas produite;		
N/A	Art. 6, 6. «incident»: un événement compromettant la disponibilité, l'authenticité, l'intégrité ou la confidentialité des données stockées, transmises ou faisant l'objet d'un traitement, ou des services que les réseaux et systèmes d'information offrent ou rendent accessibles;		
N/A	Art. 6, 7. «incident de cybersécurité majeur»: un incident qui provoque des perturbations dépassant les capacités de réaction du seul État membre concerné ou qui a un impact important sur au moins deux États membres;		

N/A	Art. 6, 8. «traitement des incidents»: toutes les actions et procédures visant à prévenir, détecter, analyser et contenir un incident ou à y répondre et à y remédier;		
N/A	Art. 6, 9. «risque»: le potentiel de perte ou de perturbation causé par un incident, à exprimer comme la combinaison de l'ampleur de cette perte ou de cette perturbation et de la probabilité qu'un tel incident se produise;		
N/A	Art. 6, 10. «cybermenace»: une cybermenace au sens de l'article 2, point 8), du règlement (UE) 2019/881;		
N/A	Art. 6, 11. «cybermenace importante»: une cybermenace qui, compte tenu de ses caractéristiques techniques, peut être considérée comme susceptible d'avoir un impact grave sur les réseaux et les systèmes d'information d'une entité ou les utilisateurs des services de l'entité, en causant un dommage		

	matériel, corporel ou moral considérable;		
N/A	Art. 6, 12. «produit TIC»: un produit TIC au sens de l'article 2, point 12), du règlement (UE) 2019/881;		
N/A	Art. 6, 13. «service TIC»: un service TIC au sens de l'article 2, point 13), du règlement (UE) 2019/881;		
N/A	Art. 6, 14. «processus TIC»: un processus TIC au sens de l'article 2, point 14), du règlement (UE) 2019/881;		
N/A	Art. 6, 15. «vulnérabilité»: une faiblesse, susceptibilité ou faille de produits TIC ou de services TIC qui peut		
N/A	Art. 6, 16. «norme»: une norme au sens de l'article 2, point 1), du règlement (UE) nº 1025/2012 du Parlement européen et du Conseil ([29]);		

N/A	Art. 6, 17. «spécification technique»: une spécification technique au sens de l'article 2, point 4), du règlement (UE) n° 1025/2012;		
N/A	Art. 6, 18. «point d'échange internet»: une structure de réseau qui permet l'interconnexion de plus de deux réseaux indépendants (systèmes autonomes), essentiellement aux fins de faciliter l'échange de trafic internet, qui n'assure l'interconnexion que pour des systèmes autonomes et qui n'exige pas que le trafic internet passant entre une paire quelconque de systèmes autonomes participants transite par un système autonome tiers, pas plus qu'il ne modifie ou n'altère par ailleurs un tel trafic;		
N/A	Art. 6, 19. «système de noms de domaine» ou «DNS»: un système hiérarchique et distribué d'affectation de noms qui permet l'identification des services et des ressources internet, ce qui rend possible l'utilisation de services de routage et de connectivité internet par les dispositifs des utilisateurs finaux pour accéder à ces services et		

	ressources;		
N/A	Art. 6, 20. «fournisseur de services DNS»: une entité qui fournit: a) des services de résolution de noms de domaine récursifs accessibles au public destinés aux utilisateurs finaux de l'internet; ou b) des services de résolution de noms de domaine faisant autorité pour une utilisation par des tiers, à l'exception des serveurs de noms de racines;		
Art. 6, 2° 2° Office d'enregistrement : une entité à laquelle un domaine de premier niveau spécifique a été délégué et qui est responsable de l'administration de ce domaine, y compris de l'enregistrement des noms de domaine en relevant et de son fonctionnement technique, notamment l'exploitation de ses serveurs de noms, la maintenance de ses bases de données et la distribution de ses fichiers de zone sur les serveurs de noms, que ces opérations soient effectuées par l'entité elle-même ou qu'elles soient sous-traitées, mais à l'exclusion des situations où les noms de domaine de premier niveau sont utilisés par un registre uniquement pour son	Art. 6, 21. «registre de noms de domaine de premier niveau»: une entité à laquelle un domaine de premier niveau spécifique a été délégué et qui est responsable de l'administration du domaine de premier niveau, y compris de l'enregistrement des noms de domaine relevant du domaine de premier niveau et du fonctionnement technique du domaine de premier niveau, notamment l'exploitation de ses serveurs de noms, la maintenance de ses bases de données et la distribution des fichiers de zone du domaine de premier niveau sur les serveurs de noms, que ces opérations soient effectuées par l'entité elle-même		Cf. Fiche d'impact « Définitions ». La définition de la directive a été recopiée dans le droit national

propre usage ;	ou qu'elles soient sous-traitées, mais à l'exclusion des situations où les noms de domaine de premier niveau sont utilisés par un registre uniquement pour son propre usage;		
Art. 6, 1° 1° Bureau d'enregistrement : une entité fournissant des services d'enregistrement de noms de domaine ;	Art. 6, 22. «entité fournissant des services d'enregistrement de noms de domaine»: un bureau d'enregistrement ou un agent agissant pour le compte de bureaux d'enregistrement, tel qu'un fournisseur ou revendeur de services d'anonymisation ou d'enregistrement fiduciaire;		Cf. Fiche d'impact « Définitions ». La définition de la directive a été recopiée dans le droit national
N/A	Art. 6, 23. «service numérique»: un service au sens de l'article 1er, paragraphe 1, point b), de la directive (UE) 2015/1535 du Parlement européen et du Conseil ([30]);		
N/A	Art. 6, 24. «service de confiance»: un service de confiance au sens de l'article 3, point 16, du règlement (UE) nº 910/2014;		
Art. 6, 3°	Art. 6, 25.		Cf. Fiche d'impact

3° Prestataire de services de confiance : un prestataire de services de confiance au sens du paragraphe 19 de l'article 3 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 ;	«prestataire de services de confiance»: un prestataire de services de confiance au sens de l'article 3, point 19, du règlement (UE) nº 910/2014 ;		« Définitions ». La définition de la directive a été recopiée dans le droit national
N/A	Art. 6, 26. «service de confiance qualifié»: un service de confiance qualifié au sens de l'article 3, point 17, du règlement (UE) nº 910/2014;		
Art. 6, 4° 4° Prestataire de service de confiance qualifié : un prestataire de services de confiance au sens du paragraphe 20 de l'article 3 du règlement (UE) no 910/2014 mentionné ci-dessus ;	Art. 6, 27. «prestataire de services de confiance qualifié»: un prestataire de services de confiance qualifié au sens de l'article 3, point 20, du règlement (UE) nº 910/2014;		Cf. Fiche d'impact « Définitions ». La définition de la directive a été recopiée dans le droit national
N/A	Art. 6, 28. «place de marché en ligne»: une place de marché en ligne au sens de l'article 2, point n), de la directive 2005/29/CE du Parlement européen et du Conseil ([31]);		

N/A	Art. 6, 29. «moteur de recherche en ligne»: un moteur de recherche en ligne au sens de l'article 2, point 5), du règlement (UE) 2019/1150 du Parlement européen et du Conseil ([32]);		
N/A	Art. 6, 30. «service d'informatique en nuage»: un service numérique qui permet l'administration à la demande et l'accès large à distance à un ensemble modulable et variable de ressources informatiques pouvant être partagées, y compris lorsque ces ressources sont réparties à différents endroits;		
Art. 6, 6° 6° Service de centre de données : un service qui englobe les structures, ou groupes de structures, dédiées à l'hébergement, l'interconnexion et l'exploitation centralisées des équipements informatiques et de réseau fournissant des services de stockage, de traitement et de transport des données, ainsi que l'ensemble des installations et infrastructures de distribution d'électricité et de contrôle environnemental ;	Art. 6, 31. «service de centre de données»: un service qui englobe les structures, ou groupes de structures, dédiées à l'hébergement, l'interconnexion et l'exploitation centralisées des équipements informatiques et de réseau fournissant des services de stockage, de traitement et de transport des données, ainsi que l'ensemble des installations et infrastructures de distribution d'électricité et de contrôle environnemental;		Cf. Fiche d'impact « Définitions ». La définition de la directive a été recopiée dans le droit national

N/A	Art. 6, 32. «réseau de diffusion de contenu»: un réseau de serveurs géographiquement répartis visant à assurer la haute disponibilité, l'accessibilité ou la fourniture rapide de contenu et de services numériques aux utilisateurs d'internet pour le compte de fournisseurs de contenu et de services;		
N/A	Art. 6, 33. «plateforme de services de réseaux sociaux»: une plateforme qui permet aux utilisateurs finaux de se connecter, de partager, de découvrir et de communiquer entre eux sur plusieurs terminaux, notamment par conversations en ligne, publications, vidéos et recommandations;		
Art. 6, 5° 5° Représentant : une personne physique ou morale établie dans l'Union qui est expressément désignée pour agir pour le compte d'un fournisseur de services de système de nom de domaine, d'un registre de noms de domaine de premier niveau, d'une entité fournissant des services d'enregistrement de noms de domaine, d'un fournisseur d'informatique en nuage, d'un fournisseur de services de centre de données, d'un fournisseur de réseau de diffusion de contenu,	Art. 6, 34. «représentant»: une personne physique ou morale établie dans l'Union qui est expressément désignée pour agir pour le compte d'un fournisseur de services DNS, d'un registre de noms de domaine de premier niveau, d'une entité fournissant des services d'enregistrement de noms de domaine, d'un fournisseur d'informatique en nuage, d'un fournisseur de services de centre de données, d'un fournisseur de réseau de diffusion de contenu, d'un		Cf. Fiche d'impact « Définitions ».

d’un fournisseur de services gérés, d’un fournisseur de services de sécurité gérés ou d’un fournisseur de places de marché en ligne, de moteurs de recherche en ligne ou de plateformes de services de réseaux sociaux non établi dans l’Union, qui peut être contactée par une autorité compétente ou un centre de veille, d'alerte et de réponse aux attaques informatiques (CERT) à la place de l’entité elle-même concernant les obligations incombant à ladite entité en vertu de la présente loi ;	fournisseur de services gérés, d’un fournisseur de services de sécurité gérés ou d’un fournisseur de places de marché en ligne, de moteurs de recherche en ligne ou de plateformes de services de réseaux sociaux non établi dans l’Union, qui peut être contactée par une autorité compétente ou un CSIRT à la place de l’entité elle-même concernant les obligations incombant à ladite entité en vertu de la présente directive;		
N/A	Art. 6, 35. «entité de l’administration publique»: une entité reconnue comme telle dans un État membre conformément au droit national, à l’exclusion de la justice, des parlements et des banques centrales, qui satisfait aux critères suivants: a) elle a été créée pour satisfaire des besoins d’intérêt général et n’a pas de caractère industriel ou commercial; b) elle est dotée de la personnalité juridique ou est juridiquement habilitée à agir pour le compte d’une autre entité dotée de la personnalité juridique; c) elle est financée majoritairement par l’État, les autorités régionales ou d’autres organismes de droit public, sa gestion est soumise à un contrôle de la part de ces		

	autorités ou organismes, ou son organe d'administration, de direction ou de surveillance est composé de membres dont plus de la moitié sont désignés par l'État, les autorités régionales ou d'autres organismes de droit public; d) elle a le pouvoir d'adresser à des personnes physiques ou morales des décisions administratives ou réglementaires affectant leurs droits en matière de mouvements transfrontières des personnes, des biens, des services ou des capitaux;		
N/A	Art. 6., 36. « réseau de communications électroniques public »: un réseau de communications électroniques public au sens de l'article 2, point 8), de la directive (UE) 2018/1972;		
N/A	Art. 6, 37. « service de communications électroniques »: un service de communications électroniques au sens de l'article 2, point 4), de la directive (UE) 2018/1972;		
N/A	Art. 6, 38. « entité »: une personne physique ou morale		

	constituée et reconnue comme telle en vertu du droit national de son lieu de constitution, et ayant, en son nom propre, la capacité d'être titulaire de droits et d'obligations;		
N/A	Art. 6, 39. « fournisseur de services gérés »: une entité qui fournit des services liés à l'installation, à la gestion, à l'exploitation ou à l'entretien de produits, de réseaux, d'infrastructures ou d'applications TIC ou d'autres réseaux et systèmes d'information, par l'intermédiaire d'une assistance ou d'une administration active, soit dans les locaux des clients, soit à distance;		
N/A	Art. 6, 40. «fournisseur de services de sécurité gérés»: un fournisseur de services gérés qui effectue ou fournit une assistance pour des activités liées à la gestion des risques en matière de cybersécurité;		
N/A	Art. 6, 41. «organisme de recherche»: une entité dont l'objectif premier est de mener des activités de recherche appliquée ou de développement expérimental en vue d'exploiter les résultats de		

	cette recherche à des fins commerciales, à l'exclusion des établissements d'enseignement.		
N/A	Art. 7, 1. 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. La stratégie nationale en matière de cybersécurité comprend: a) les objectifs et priorités de la stratégie de l'État membre en matière de cybersécurité, couvrant en particulier les secteurs visés aux annexes I et II; b) un cadre de gouvernance visant à atteindre les objectifs et priorités visés au point a) du présent paragraphe, y compris les politiques visées au paragraphe 2; c) un cadre de gouvernance précisant les rôles et les responsabilités des parties prenantes concernées au niveau national, et sur lequel reposent la coopération et la coordination au niveau national entre les autorités compétentes, les points de contact uniques et les CSIRT en vertu de la présente directive, ainsi que la		La revue stratégique de cyberdéfense (Revue stratégique de cyberdéfense | SGDSN) est en cours de mise à jour et prévoit de prendre en compte les dispositions prévues dans la directive NIS 2. Cette mise à jour devrait être publiée en 2024

	coordination et la coopération entre ces organismes et les autorités compétentes en vertu d'actes juridiques sectoriels de l'Union; d) un mécanisme visant à déterminer les actifs pertinents et une évaluation des risques dans cet État membre; e) un inventaire des mesures garantissant la préparation, la réaction et la récupération des services après incident, y compris la coopération entre les secteurs public et privé; f) une liste des différents acteurs et autorités concernés par la mise en œuvre de la stratégie nationale en matière de cybersécurité; g) un cadre politique visant une coordination renforcée entre les autorités compétentes en vertu de la présente directive et de la directive (UE) 2022/2557 aux fins du partage d'informations relatives aux risques, aux menaces et aux incidents dans les domaines cyber et non cyber et de l'exercice des tâches de supervision, le cas échéant; h) un plan comprenant les mesures nécessaires en vue d'améliorer le niveau général de sensibilisation des citoyens à la cybersécurité.		
N/A	Art. 7, 2. Dans le cadre de la stratégie nationale en matière		La revue stratégique de cyberdéfense (Revue stratégique de

	de cybersécurité, les États membres adoptent notamment des politiques portant sur les éléments suivants: a) la cybersécurité dans le cadre de la chaîne d'approvisionnement des produits et services TIC utilisés par des entités pour la fourniture de leurs services; b) l'inclusion et la spécification d'exigences liées à la cybersécurité pour les produits et services TIC dans les marchés publics, y compris concernant la certification de cybersécurité, le chiffrement et l'utilisation de produits de cybersécurité en sources ouvertes; c) la gestion des vulnérabilités, y compris la promotion et la facilitation de la divulgation coordonnée des vulnérabilités en vertu de l'article 12, paragraphe 1; d) le maintien de la disponibilité générale, de l'intégrité et de la confidentialité du noyau public de l'internet ouvert, y compris, le cas échéant, la cybersécurité des câbles de communication sous-marins; e) la promotion du développement et de l'intégration de technologies avancées pertinentes visant à mettre en œuvre des mesures de pointe dans la gestion des risques en matière de cybersécurité;		cyberdéfense | SGDSN) est en cours de mise à jour et prévoit de prendre en compte les dispositions prévues dans la directive NIS 2. Cette mise à jour devrait être publiée en 2024

	f) la promotion et le développement de l'éducation et de la formation en matière de cybersécurité, des compétences 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'intention des citoyens, des parties prenantes et des entités; g) le soutien aux institutions universitaires et de recherche visant à développer, améliorer et promouvoir le déploiement des outils de cybersécurité et à sécuriser les infrastructures de réseau; h) la mise en place de procédures pertinentes et d'outils de partage d'informations appropriés visant à soutenir le partage volontaire d'informations sur la cybersécurité entre les entités conformément au droit de l'Union; i) le renforcement des valeurs de cyberrésilience et de cyberhygiène des petites et moyennes entreprises, en particulier celles qui sont exclues du champ d'application de la présente directive, en fournissant des orientations et un soutien facilement accessibles pour répondre à leurs besoins spécifiques; j) la promotion d'une cyberprotection active.		

N/A	Art. 7, 3. Les États membres notifient leur stratégie nationale en matière de cybersécurité à la Commission dans un délai de trois mois suivant leur adoption. Les États membres peuvent exclure de ces notifications les informations relatives à leur sécurité nationale.		
N/A	Art. 7, 4. Les États membres évaluent régulièrement leur stratégie nationale en matière de cybersécurité, et au moins tous les cinq ans, sur la base d'indicateurs clés de performance et, le cas échéant, les modifient. L'ENISA aide les États membres, à leur demande, à élaborer ou actualiser une stratégie nationale en matière de cybersécurité et des indicateurs clés de performance aux fins de l'évaluation de cette stratégie, afin de l'aligner sur les exigences et les obligations prévues par la présente directive.		
Art. 5 L'autorité nationale de sécurité des systèmes d'information est chargée de la mise en œuvre de la politique du Gouvernement en matière de sécurité des systèmes d'information régie par le présent titre et de son contrôle.	Art. 8, 1. Chaque État membre désigne ou établit une ou plusieurs autorités compétentes chargées de la cybersécurité et des tâches de supervision visées au chapitre VII (ci-après dénommées « autorités	Norme de niveau législatif, qui sera à décliner par un décret.	Cf. Fiche d'impact « Missions et compétences de l'autorité nationale ». En France, l'agence nationale de sécurité des

Le Premier ministre peut désigner un organisme autre que l'autorité nationale de sécurité des systèmes d'information mentionnée au premier alinéa pour exercer à l'égard de certaines entités, à raison de leur activité dans le domaine de la défense, certaines des responsabilités de cette autorité prévues par le présent titre. Les missions de l'autorité nationale et des organismes désignés par le Premier ministre ainsi que leurs conditions d'exercice sont précisées par décret en Conseil d'Etat.	compétentes »).		systèmes d'information sera l'autorité nationale cheffe de file au titre de la directive NIS 2.
Art. 26, 3° Les agents et personnes, spécialement désignés et assermentés à cet effet, de l'autorité nationale de sécurité des systèmes d'information, des organismes indépendants ou d'autres services de l'Etat qu'elle désigne sont habilités à rechercher et à constater les manquements et infractions aux obligations prévues par : 3° Le chapitre II et III de la présente loi ;	Art. 8, 2. Les autorités compétentes visées au paragraphe 1 contrôlent la mise en œuvre de la présente directive au niveau national.		Cf. Fiche d'impact « Supervision – Procédures de contrôle et de sanction ».
Art. 5 L'autorité nationale de sécurité des systèmes d'information est chargée de la mise en œuvre de la politique du Gouvernement en matière de sécurité des systèmes d'information régie par le présent titre et de	Art. 8, 3. Chaque État membre désigne ou établit un point de contact unique. Lorsqu'un État membre désigne ou établit une seule autorité compétente conformément au paragraphe 1, cette dernière fait	Norme de niveau législatif, qui sera à décliner par	En France, l'agence nationale de sécurité des systèmes d'information sera l'autorité nationale cheffe de file au titre de

son contrôle. Le Premier ministre peut désigner un organisme autre que l'autorité nationale de sécurité des systèmes d'information mentionnée au premier alinéa pour exercer à l'égard de certaines entités, à raison de leur activité dans le domaine de la défense, certaines des responsabilités de cette autorité prévues par le présent titre. Les missions de l'autorité nationale et des organismes désignés par le Premier ministre ainsi que leurs conditions d'exercice sont précisées par décret en Conseil d'Etat.	aussi fonction de point de contact unique dudit État membre.	un décret.	la directive NIS 2.
Art. 23 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'autorité nationale de sécurité des systèmes d'information, et, d'autre part, la Commission nationale de l'informatique et des libertés 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	Art. 8, 4. Chaque point de contact unique exerce une fonction de liaison visant à assurer la coopération transfrontière des autorités de son État membre avec les autorités compétentes des autres États membres et, le cas échéant, avec la Commission et l'ENISA, ainsi qu'à garantir la coopération intersectorielle avec les autres autorités compétentes de son État membre.	Norme de niveau législatif, qui sera à décliner par un décret.	Cf. Fiche d'impact « Notifications d'incidents importants et partage d'informations ».

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 Etats membres de l'Union européenne ou des centres de réponse aux incidents de sécurité informatique ou des organismes internationaux concourant aux missions de sécurité ou de défense des systèmes d'information. Les modalités d'application du présent article, notamment les modalités du partage d'informations, sont déterminées par décret en Conseil d'Etat.			
N/A	Art. 8, 5. Les États membres veillent à ce que leurs autorités compétentes et points de contact uniques disposent de ressources suffisantes pour pouvoir s'acquitter de leurs tâches de manière effective et efficace et atteindre ainsi les objectifs de la présente directive.		
Art. 5 L'autorité nationale de sécurité des systèmes d'information est chargée de la mise en œuvre de la politique du Gouvernement en matière de sécurité des systèmes d'information régie par le présent titre et de son contrôle. Le Premier ministre peut désigner un organisme autre que l'autorité nationale de sécurité des systèmes	Art. 8, 6. Chaque État membre notifie à la Commission, sans retard injustifié, l'identité de l'autorité compétente visée au paragraphe 1 et du point de contact unique visé au paragraphe 3, les tâches qui sont confiées à ces autorités et toute modification ultérieure dans ce cadre. Chaque État membre rend publique l'identité de son autorité compétente. La Commission publie une liste des points de contact	Norme de niveau législatif, qui sera à décliner par un décret.	Cf. Fiche d'impact « Missions et compétences de l'autorité nationale ».

d'information mentionnée au premier alinéa pour exercer à l'égard de certaines entités, à raison de leur activité dans le domaine de la défense, certaines des responsabilités de cette autorité prévues par le présent titre. Les missions de l'autorité nationale et des organismes désignés par le Premier ministre ainsi que leurs conditions d'exercice sont précisées par décret en Conseil d'Etat.	uniques.		
Art. 5 L'autorité nationale de sécurité des systèmes d'information est chargée de la mise en œuvre de la politique du Gouvernement en matière de sécurité des systèmes d'information régie par le présent titre et de son contrôle. Le Premier ministre peut désigner un organisme autre que l'autorité nationale de sécurité des systèmes d'information mentionnée au premier alinéa pour exercer à l'égard de certaines entités, à raison de leur activité dans le domaine de la défense, certaines des responsabilités de cette autorité prévues par le présent titre. Les missions de l'autorité nationale et des organismes désignés par le Premier ministre ainsi que leurs conditions d'exercice sont précisées par décret en Conseil d'Etat.	<u>Art. 9, 1.</u> Chaque État membre désigne ou établit une ou plusieurs autorités compétentes qui sont chargées de la gestion des incidents de cybersécurité majeurs et des crises (ci-après dénommées « autorités de gestion des crises cyber »). Les États membres veillent à ce que ces autorités disposent de ressources suffisantes pour s'acquitter, de manière effective et efficace, des tâches qui leur sont dévolues. Les États membres veillent à la cohérence avec les cadres nationaux existants pour la gestion générale des crises.	Norme de niveau législatif, qui sera à décliner par un décret.	Cf. Fiche d'impact « Missions et compétences de l'autorité nationale ».

N/A	Art. 9, 2. Lorsqu'un État membre désigne ou établit plus d'une autorité de gestion des crises cyber conformément au paragraphe 1, il indique clairement laquelle de ces autorités fera office de coordinateur pour la gestion des incidents de cybersécurité majeurs et des crises.		
N/A	Art. 9, 3. Chaque État membre recense les capacités, les moyens et les procédures qui peuvent être déployés en cas de crise aux fins de la présente directive.		
N/A	Art. 9, 4. Chaque État membre adopte un plan national de réaction aux crises et incidents de cybersécurité majeurs dans lequel sont définis les objectifs et les modalités de gestion des incidents de cybersécurité majeurs et des crises. Ce plan établit notamment les éléments suivants: a) les objectifs des mesures et activités nationales de préparation; b) les tâches et responsabilités des autorités de gestion des crises cyber; c) les procédures de gestion des crises cyber, y		La France a doté son plan Vigipirate d'un volet numérique pour définir une posture de vigilance permanente dans le cyber espace. De plus, la France s'est dotée d'un plan PIRANET qui permet définir les modalités de réponse de l'État en cas d'agression cyber + incident IT, c'est un

	compris leur intégration dans le cadre national général de gestion des crises et les canaux d'échange d'informations; d) les mesures de préparation nationales, y compris des exercices et des activités de formation; e) les parties prenantes et les infrastructures des secteurs public et privé concernées; f) les procédures et arrangements nationaux entre les autorités et les organismes nationaux compétents visant à garantir la participation et le soutien effectifs de l'État membre à la gestion coordonnée des incidents de cybersécurité majeurs et des crises au niveau de l'Union.		document NP qui a été signé par le cabinet du PM l'année dernière. Ce document vient en complément du volet numérique du plan Vigipirate dans une logique d'escalade si on a besoin d'activer des mesures complémentaires.
N/A	<u>Art. 9, 5.</u> Dans un délai de trois mois à compter de la désignation ou de la mise en place de l'autorité de gestion des crises cyber visée au paragraphe 1, chaque État membre notifie à la Commission l'identité de son autorité et toute modification ultérieure dans ce cadre. Les États membres soumettent à la Commission et au réseau européen pour la préparation et la gestion des crises cyber (EU-CyCLONe) les informations pertinentes relatives aux prescriptions du paragraphe 4 concernant leurs plans nationaux d'intervention en cas d'incident de cybersécurité majeurs et de crise		

	dans un délai de trois mois suivant l'adoption de ces plans. Les États membres peuvent exclure certaines informations si et dans la mesure où cette exclusion est nécessaire pour préserver la sécurité nationale.		
Art. 5 L'autorité nationale de sécurité des systèmes d'information est chargée de la mise en œuvre de la politique du Gouvernement en matière de sécurité des systèmes d'information régie par le présent titre et de son contrôle. Le Premier ministre peut désigner un organisme autre que l'autorité nationale de sécurité des systèmes d'information mentionnée au premier alinéa pour exercer à l'égard de certaines entités, à raison de leur activité dans le domaine de la défense, certaines des responsabilités de cette autorité prévues par le présent titre. Les missions de l'autorité nationale et des organismes désignés par le Premier ministre ainsi que leurs conditions d'exercice sont précisées par décret en Conseil d'Etat.	<u>Art. 10, 1.</u> Chaque État membre désigne ou met en place un ou plusieurs CSIRT. Les CSIRT peuvent être désignés ou établis au sein d'une autorité compétente. Les CSIRT se conforment aux exigences énumérées à l'article 11, paragraphe 1, couvrent au moins les secteurs, les sous-secteurs et les types d'entités visés aux annexes I et II, et sont chargés de la gestion des incidents selon un processus bien défini.	Norme de niveau législatif, qui sera à décliner par un décret.	Cf. Fiche d'impact « Missions et compétences de l'autorité nationale ».
N/A	<u>Art. 10, 2.</u> Les États membres veillent à ce que chaque CSIRT dispose de ressources suffisantes pour pouvoir		

	s'acquitter efficacement de ses tâches énumérées à l'article 11, paragraphe 3.		
Article 24 L'autorité nationale de sécurité des systèmes d'information agrée des organismes publics ou privés en tant que relais dans la prévention et la gestion des incidents. L'autorité et les organismes qu'elle a ainsi agréés sont autorisés à échanger entre eux des informations couvertes par des secrets protégés par la loi. Les modalités d'application du présent article, notamment les modalités de dépôt et d'examen des demandes d'agrément des organismes mentionnés au premier alinéa, sont déterminées par décret en Conseil d'Etat.	Art. 10, 3. Les États membres veillent à ce que chaque CSIRT dispose d'une infrastructure de communication et d'information adaptée, sécurisée et résiliente leur permettant d'échanger des informations avec les entités essentielles et importantes et les autres parties prenantes. À cette fin, les États membres veillent à ce que chaque CSIRT contribue au déploiement d'outils sécurisés de partage d'informations.	Norme de niveau législatif, qui sera à décliner par un décret.	Cf. Fiche d'impact « Notification d'incidents et partage d'informations ».
N/A	Art. 10, 4. Les CSIRT coopèrent et, le cas échéant, échangent des informations pertinentes conformément à l'article 29 avec des communautés sectorielles ou intersectorielles d'entités essentielles et importantes.		Cf. Fiche d'impact « Notification d'incidents et partage d'informations ».
N/A	Art. 10, 5. Les CSIRT participent aux évaluations par les pairs		

	organisées conformément à l'article 19.		
N/A	Art. 10, 6. Les États membres veillent à ce que leurs CSIRT coopèrent de manière effective, efficace et sécurisée au sein du réseau des CSIRT.		
N/A	Art. 10, 7. Les CSIRT peuvent établir des relations de coopération avec les centres de réponse aux incidents de sécurité informatique nationaux de pays tiers. Dans le cadre de ces relations de coopération, les États membres facilitent un échange d'informations effectif, efficace et sécurisé avec ces centres de réponse aux incidents de sécurité informatique nationaux de pays tiers, en utilisant les protocoles d'échange d'informations appropriés, y compris le «Traffic Light Protocol». Les CSIRT peuvent échanger des informations pertinentes avec des centres de réponse aux incidents de sécurité informatique nationaux de pays tiers, y compris des données à caractère personnel, dans le respect du droit de l'Union en matière de protection des données.		Cf. Fiche d'impact « Notification d'incidents et partage d'informations ».
N/A	Art. 10, 8.		Cf. Fiche d'impact « Notification

	Les CSIRT peuvent coopérer avec des centres de réponse aux incidents de sécurité informatique nationaux de pays tiers ou des organismes équivalents de pays tiers, notamment dans le but de leur fournir une assistance en matière de cybersécurité.		d'incidents et partage d'informations ».
N/A	Art. 10, 9. Chaque État membre notifie à la Commission, sans retard injustifié, l'identité des CSIRT visés au paragraphe 1 du présent article et du CSIRT désigné comme coordinateur conformément à l'article 12, paragraphe 1, leurs tâches respectives à l'égard des entités essentielles et importantes, et toute modification ultérieure dans ce cadre.		
N/A	Art. 10, 10. Les États membres peuvent solliciter l'assistance de l'ENISA pour la mise en place de leurs CSIRT.		
Art. 24 Les modalités d'application du présent article, notamment les modalités de dépôt et d'examen des demandes d'agrément des organismes mentionnés au premier alinéa, sont déterminées par décret en Conseil d'Etat.	Art. 11, 1. Les CSIRT satisfont aux exigences suivantes: a) les CSIRT veillent à un niveau élevé de disponibilité de leurs canaux de communication en évitant les points uniques de défaillance et	Norme de niveau législatif, qui sera à décliner par un décret.	Cf. Fiche d'impact « Notification d'incidents et partage d'informations ».

	disposent de plusieurs moyens pour être contactés et contacter autrui à tout moment; ils spécifient clairement les canaux de communication et les font connaître aux partenaires et collaborateurs; b) les locaux des CSIRT et les systèmes d'information utilisés se trouvent sur des sites sécurisés; c) les CSIRT sont dotés d'un système approprié de gestion et de routage des demandes afin, notamment, de faciliter les transferts effectifs et efficaces; d) les CSIRT garantissent la confidentialité et la fiabilité de leurs opérations; e) les CSIRT sont dotés des effectifs adéquats afin de pouvoir garantir une disponibilité permanente de leurs services et ils veillent à ce que leur personnel reçoive une formation appropriée; f) les CSIRT sont dotés de systèmes redondants et d'un espace de travail de secours pour assurer la continuité de leurs services. Les CSIRT peuvent participer à des réseaux de coopération internationale.		
N/A	Art. 11, 2.		

	Les États membres veillent à ce que leurs CSIRT disposent conjointement des capacités techniques nécessaires pour pouvoir s'acquitter des tâches visées au paragraphe 3. Les États membres veillent à ce que des ressources suffisantes soient allouées à leurs CSIRT pour garantir des effectifs suffisants leur permettant de développer leurs capacités techniques.		
Art. 5 L'autorité nationale de sécurité des systèmes d'information est chargée de la mise en œuvre de la politique du Gouvernement en matière de sécurité des systèmes d'information régie par le présent titre et de son contrôle. Le Premier ministre peut désigner un organisme autre que l'autorité nationale de sécurité des systèmes d'information mentionnée au premier alinéa pour exercer à l'égard de certaines entités, à raison de leur activité dans le domaine de la défense, certaines des responsabilités de cette autorité prévues par le présent titre. Les missions de l'autorité nationale et des organismes désignés par le Premier ministre ainsi que leurs conditions d'exercice sont précisées par décret en Conseil d'Etat.	Art. 11, 3. 2) Les CSIRT assument les tâches suivantes: i. surveiller et analyser les cybermenaces, les vulnérabilités et les incidents au niveau national et, sur demande, apporter une assistance aux entités essentielles et importantes concernées pour surveiller en temps réel ou quasi réel leurs réseaux et systèmes d'information; ii. activer le mécanisme d'alerte précoce, la diffusion de messages d'alerte, les annonces et la diffusion d'informations sur les cybermenaces, les vulnérabilités et les incidents auprès des entités essentielles et importantes concernées ainsi qu'auprès des autorités compétentes et des autres parties prenantes concernées, si possible en temps quasi réel; iii. réagir aux incidents et apporter une assistance aux entités essentielles et importantes	Norme de niveau législatif, qui sera à décliner par un décret.	Cf. Fiche d'impact « Missions et compétences de l'autorité nationale ».

	concernées, le cas échéant; iv. rassembler et analyser des données de police scientifique, et assurer une analyse dynamique des risques et incidents et une appréciation de la situation en matière de cybersécurité; v. réaliser, à la demande d'une entité essentielle ou importante, un scan proactif du réseau et des systèmes d'information de l'entité concernée afin de détecter les vulnérabilités susceptibles d'avoir un impact important; vi. participer au réseau des CSIRT et apporter une assistance mutuelle en fonction de leurs capacités et de leurs compétences aux autres membres du réseau des CSIRT à leur demande; vii. le cas échéant, agir en qualité de coordinateur aux fins du processus de divulgation coordonnée des vulnérabilités en vertu de l'article 12, paragraphe 1; viii. contribuer au déploiement d'outils de partage d'informations sécurisés conformément à l'article 10, paragraphe 3. Les CSIRT peuvent procéder à un scan proactif et non intrusif des réseaux et systèmes d'information accessibles au public d'entités essentielles et importantes. Ce scan est effectué dans le but de détecter les réseaux et systèmes d'information vulnérables ou configurés de façon peu sûre et d'informer les entités concernées. Ce scan n'a pas		

	d'effet négatif sur le fonctionnement des services des entités. Lorsqu'ils exécutent les tâches visées au premier alinéa, les CSIRT peuvent donner la priorité à certaines tâches sur la base d'une approche basée sur les risques.		
N/A	Art. 11, 4. Les CSIRT établissent des relations de coopération avec les acteurs concernés du secteur privé, en vue d'atteindre les objectifs de la présente directive.		Cf. Fiche d'impact « Notification d'incidents et partage d'informations ». Le choix du CSIRT national et gouvernemental pour la France au titre de la directive NIS 2 sera prévu par décret du Conseil d'Etat. C'est le CERT-FR, qui est sous la responsabilité de l'agence nationale de sécurité des systèmes d'information, autorité nationale de sécurité des systèmes d'information au titre de l'article R. 2321-1 du code de la défense, qui sera

			désigné.
N/A	Art. 11, 5. Afin de faciliter la coopération visée au paragraphe 4, les CSIRT encouragent l'adoption et l'utilisation de pratiques, de systèmes de classification et de taxonomies communs ou normalisés en ce qui concerne: a) les procédures de gestion des incidents; b) la gestion de crise; et c) la divulgation coordonnée des vulnérabilités en vertu de l'article 12, paragraphe 1.		
N/A	Art. 12, 1. Chaque État membre désigne l'un de ses CSIRT comme coordinateur aux fins de la divulgation coordonnée des vulnérabilités. Le CSIRT désigné comme coordinateur fait office d'intermédiaire de confiance en facilitant, si nécessaire, les interactions entre la personne physique ou morale qui signale une vulnérabilité et le fabricant ou le fournisseur des produits TIC ou des services TIC potentiellement vulnérables, à la demande de l'une des deux parties. Les tâches du CSIRT désigné comme coordinateur consistent: a) à identifier et contacter les entités		Cf. Fiche d'impact « Notification d'incidents et partage d'informations ». A noter que la France, dans le cadre de la loi de programmation militaire 2024 – 2030 a codifié dans le code de la défense, à l'article L. 2321-4-1, l'obligation, pour les éditeurs de logiciel, de notifier l'autorité nationale de

	concernées; b) à apporter une assistance aux personnes physiques ou morales signalant une vulnérabilité; et c) à négocier des délais de divulgation et gérer les vulnérabilités qui touchent plusieurs entités. Les États membres veillent à ce que les personnes physiques ou morales soient en mesure de signaler une vulnérabilité, de manière anonyme lorsqu'elles le demandent, au CSIRT désigné comme coordinateur. Le CSIRT désigné comme coordinateur veille à ce que des mesures de suivi diligentes soient prises en ce qui concerne la vulnérabilité signalée et veille à l'anonymat de la personne physique ou morale signalant la vulnérabilité. Lorsque la vulnérabilité signalée est susceptible d'avoir un impact important sur des entités dans plusieurs États membres, le CSIRT désigné comme coordinateur de chaque État membre concerné coopère, le cas échéant, avec les autres CSIRT désignés comme coordinateurs au sein du réseau des CSIRT.		sécurité des systèmes d'information en cas de vulnérabilité significative affectant un de leurs produits ou en cas d'incident informatique compromettant la sécurité de leurs systèmes d'information et susceptible d'affecter significativement un de leurs produits
N/A	Art. 12, 2. L'ENISA élabore et tient à jour, après consultation du groupe de coopération, une base de données européenne des vulnérabilités. À cette fin, l'ENISA		

	établit et gère les systèmes d'information, les politiques et les procédures appropriés, et adopte les mesures techniques et organisationnelles nécessaires pour assurer la sécurité et l'intégrité de la base de données européenne des vulnérabilités, en vue notamment de permettre aux entités, indépendamment du fait qu'elles relèvent ou non du champ d'application de la présente directive, et à leurs fournisseurs de réseaux et de systèmes d'information, de divulguer et d'enregistrer, à titre volontaire, les vulnérabilités publiquement connues présentes dans les produits TIC ou les services TIC. Toutes les parties prenantes ont accès aux informations sur les vulnérabilités contenues dans la base de données européenne sur les vulnérabilités. Cette base de données comprend: a) des informations décrivant la vulnérabilité; b) les produits TIC ou les services TIC affectés ainsi que la gravité de la vulnérabilité rapportée aux circonstances dans lesquelles elle peut être exploitée; c) la disponibilité des correctifs correspondants et, en l'absence de correctifs disponibles, des orientations fournies par les autorités compétentes ou les CSIRT, adressées aux utilisateurs des produits TIC et des services TIC vulnérables, sur la manière dont les risques résultant des vulnérabilités divulguées peuvent		

	être atténués.		
N/A	Art. 13, 1. Lorsqu'ils sont distincts, les autorités compétentes, le point de contact unique et les CSIRT d'un même État membre coopèrent les uns avec les autres afin de respecter les obligations énoncées dans la présente directive.		
Art. 17 Les personnes mentionnées à l'article 14 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.	Art. 13, 2. Les États membres veillent à ce que leurs CSIRT ou, le cas échéant, leurs autorités compétentes reçoivent les notifications relatives aux incidents importants conformément à l'article 23, et aux incidents, aux cybermenaces et aux incidents évités conformément à l'article 30.		Cf. Fiche d'impact « Notification d'incidents et partage d'informations ».
N/A	Art. 13, 3. Les États membres veillent à ce que leurs CSIRT ou, le cas échéant, leurs autorités compétentes informent leurs points de contact uniques des notifications d'incidents, de cybermenaces et d'incidents évités soumises en application de la présente directive.		En France, l'autorité compétente, le CSIRT et le point de contact unique sont des responsabilités assumées par l'autorité nationale de sécurité des systèmes d'information, sauf pour certaines activités dans le domaine de la défense, où cette

			responsabilité sera confiée à d'autres organismes désignés par le Premier ministre.
Art. 23 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'autorité nationale de sécurité des systèmes d'information, et, d'autre part, la Commission nationale de l'informatique et des libertés 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 Etats membres de l'Union européenne ou des centres de réponse aux incidents de sécurité informatique ou des organismes internationaux concourant aux missions de sécurité ou de défense des systèmes d'information. Les modalités d'application du présent article,	<u>Art. 13, 4.</u> Afin de veiller à ce que les tâches et obligations des autorités compétentes, des points de contact uniques et des CSIRT soient exécutées efficacement, les États membres assurent, dans la mesure du possible, une coopération appropriée entre ces organes et les autorités répressives, les autorités chargées de la protection des données, les autorités nationales en vertu des règlements (CE) n° 300/2008 et (UE) 2018/1139, les organes de contrôle au titre du règlement (UE) n° 910/2014, les autorités compétentes en vertu du règlement (UE) 2022/2554, les autorités de régulation nationales en vertu de la directive (UE) 2018/1972, les autorités compétentes en vertu de la directive (UE) 2022/2557, ainsi que les autorités compétentes en vertu d'autres actes juridiques sectoriels de l'Union, dans cet État membre.		Cf. Fiche d'impact « Notification d'incidents et partage d'informations ».

notamment les modalités du partage d'informations, sont déterminées par décret en Conseil d'Etat.			
N/A	Art. 13, 5. Les États membres veillent à ce que leurs autorités compétentes en vertu de la présente directive et leurs autorités compétentes en vertu de la directive (UE) 2022/2557 coopèrent et échangent régulièrement des informations sur le recensement des entités critiques, les risques, les cybermenaces et les incidents, ainsi que sur les risques, menaces et incidents non cyber qui touchent les entités essentielles recensées en tant qu'entités critiques en vertu de la directive (UE) 2022/2557, et sur les mesures prises pour faire face à ces risques, menaces et incidents. Les États membres veillent également à ce que leurs autorités compétentes en vertu de la présente directive et leurs autorités compétentes en vertu du règlement (UE) n° 910/2014, du règlement (UE) 2022/2554 et de la directive (UE) 2018/1972 échangent régulièrement des informations pertinentes, y compris en ce qui concerne les incidents et les cybermenaces concernés.		
Art. 17 Un décret en Conseil d'Etat fixe les modalités d'application du présent article. Il précise notamment	Art. 13, 6. Les États membres simplifient la communication d'informations par des moyens techniques pour les	Norme de niveau législatif, qui sera à	Cf. Fiche d'impact « Notification d'incidents et partage

la procédure applicable et les critères d'appréciation des caractères importants et critiques des incidents et vulnérabilités ainsi que les délais de notification des incidents et des vulnérabilités.	notifications visées aux articles 23 et 30.	décliner par un décret.	d'informations ».
N/A	Art. 14, 1. Un groupe de coopération est institué afin de soutenir et de faciliter la coopération stratégique et l'échange d'informations entre les États membres et de renforcer la confiance.		
N/A	Art. 14, 2. Le groupe de coopération exécute ses tâches en s'appuyant sur les programmes de travail bisannuels visés au paragraphe 7.		
N/A	Art. 14, 3. Le groupe de coopération est composé de représentants des États membres, de la Commission et de l'ENISA. Le Service européen pour l'action extérieure participe aux activités du groupe de coopération en qualité d'observateur. Les autorités européennes de surveillance (AES) et les autorités compétentes en vertu du règlement (UE) 2022/2554 peuvent participer aux activités du groupe de coopération conformément à l'article 47,		

	paragraphe 1, dudit règlement. Si besoin est, le groupe de coopération peut inviter le Parlement européen et des représentants des acteurs concernés à participer à ses travaux. Le secrétariat est assuré par la Commission.		
N/A	<u>Art. 14, 4.</u> 1) Le groupe de coopération est chargé des tâches suivantes: a) la fourniture d'orientations aux autorités compétentes en rapport avec la transposition et la mise en œuvre de la présente directive; b) la fourniture d'orientations aux autorités compétentes en ce qui concerne l'élaboration et la mise en œuvre des politiques de divulgation coordonnée des vulnérabilités visées à l'article 7, paragraphe 2, point c); c) l'échange des meilleures pratiques et d'informations relatives à la mise en œuvre de la présente directive, notamment en ce qui concerne les cybermenaces, les incidents, les vulnérabilités, les incidents évités, les initiatives de sensibilisation, les formations, les exercices et les compétences, le renforcement des		

	capacités, les normes et les spécifications techniques ainsi que l'identification des entités essentielles et importantes en vertu de l'article 2, paragraphe 2, points b) à e); d) l'échange de conseils et la coopération avec la Commission sur les initiatives politiques émergentes en matière de cybersécurité et la cohérence globale des exigences sectorielles en matière de cybersécurité; e) l'échange de conseils et la coopération avec la Commission sur les projets d'actes délégués ou d'actes d'exécution adoptés en vertu de la présente directive; f) l'échange de bonnes pratiques et d'informations avec les institutions, organes et organismes compétents de l'Union; g) l'échange de vues sur la mise en œuvre d'actes juridiques sectoriels de l'Union contenant des dispositions en matière de cybersécurité; h) le cas échéant, la discussion portant sur les rapports relatifs à l'évaluation par les pairs visés à l'article 19, paragraphe 9, et l'élaboration de conclusions et de recommandations; i) la réalisation d'évaluations coordonnées des risques pour la sécurité des chaînes d'approvisionnement critiques, conformément à l'article 22, paragraphe 1; j) la discussion portant sur les cas d'assistance		

	mutuelle, y compris les expériences et les résultats des activités de contrôle transfrontières visées à l'article 37; k) à la demande d'un ou de plusieurs États membres concernés, la discussion portant sur les demandes spécifiques d'assistance mutuelle visées à l'article 37; l) l'indication d'une orientation stratégique au réseau des CSIRT et au réseau UE-CyCLONe sur des questions spécifiques émergentes; m) l'échange de vues sur la politique relative aux mesures prises à la suite d'incidents de cybersécurité majeurs et de crises, sur la base des enseignements tirés du réseau des CSIRT et d'EU-CyCLONe; n) la contribution aux capacités en matière de cybersécurité dans l'ensemble de l'Union via la facilitation de l'échange de fonctionnaires nationaux grâce à un programme de renforcement des capacités impliquant le personnel des autorités compétentes ou des CSIRT; o) l'organisation régulière de réunions conjointes avec les parties intéressées privées, de toute l'Union, en vue de discuter des activités menées par le groupe de coopération et de recueillir des informations sur les nouveaux défis politiques; p) la discussion portant sur les travaux		

	entrepris en relation avec les exercices de cybersécurité, y compris les travaux effectués par l'ENISA; q) la mise au point de la méthodologie et des aspects organisationnels des évaluations par les pairs visées à l'article 19, paragraphe 1, ainsi que la définition de la méthode d'autoévaluation pour les États membres conformément à l'article 19, paragraphe 4, avec l'aide de la Commission et de l'ENISA, et l'élaboration, en coopération avec la Commission et l'ENISA, des codes de conduite sous-tendant les méthodes de travail des experts en cybersécurité désignés conformément à l'article 19, paragraphe 6; r) l'élaboration, aux fins de la révision visée à l'article 40, de rapports sur l'expérience acquise au niveau stratégique et à partir des évaluations par les pairs; s) l'examen et l'évaluation, de manière régulière, de l'état de la situation en matière de cybermenaces ou d'incidents, comme les rançongiciels. Le groupe de coopération soumet les rapports visés au premier alinéa, point r), à la Commission, au Parlement européen et au Conseil.		

N/A	Art. 14, 5. Les États membres font en sorte que leurs représentants au sein du groupe de coopération puissent coopérer de manière effective, efficace et sécurisée.		
N/A	Art. 14, 6. Le groupe de coopération peut demander au réseau des CSIRT d'élaborer un rapport technique sur des sujets choisis.		
N/A	Art. 14, 7. Au plus tard le 1er février 2024, puis tous les deux ans, le groupe de coopération établit un programme de travail concernant les actions à entreprendre pour mettre en œuvre ses objectifs et ses tâches.		
N/A	Art. 14, 8. La Commission peut adopter des actes d'exécution fixant les modalités de procédure nécessaires au fonctionnement du groupe de coopération. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 39,		

	paragraphe 2. La Commission échange des conseils et coopère avec le groupe de coopération sur les projets d'actes d'exécution visés au premier alinéa du présent paragraphe conformément au paragraphe 4, point e).		
N/A	Art. 14, 9. Le groupe de coopération se réunit régulièrement et en tout état de cause au moins une fois par an avec le groupe sur la résilience des entités critiques institué par la directive (UE) 2022/2557 afin de promouvoir et de faciliter la coopération stratégique et l'échange d'informations.		
N/A	Art. 15, 1. Un réseau des CSIRT nationaux est institué afin de contribuer au renforcement de la confiance et de promouvoir une coopération opérationnelle rapide et effective entre les États membres.		
N/A	Art. 15, 2. Le réseau des CSIRT est composé de représentants des CSIRT, désignés ou mis en place en vertu de l'article 10, et de l'équipe d'intervention en cas		

	d'urgence informatique pour les institutions, organes et agences de l'Union (CERT-UE). La Commission participe au réseau des CSIRT en qualité d'observateur. L'ENISA assure le secrétariat et apporte une aide active à la coopération entre les CSIRT.		
N/A	Art. 15, 3. 1) Le réseau des CSIRT est chargé des tâches suivantes: a) l'échange d'informations sur les capacités des CSIRT; b) la facilitation du partage, du transfert et de l'échange, entre les CSIRT, des technologies et des mesures, politiques, outils, processus, meilleures pratiques et cadres pertinents; c) l'échange d'informations pertinentes sur les incidents, les incidents évités, les cybermenaces, les risques et les vulnérabilités; d) l'échange d'informations en ce qui concerne les publications et les recommandations en matière de cybersécurité; e) l'assurance de l'interopérabilité en ce qui concerne les spécifications et les protocoles relatifs au partage d'informations; f) à la demande d'un membre du réseau des		

	CSIRT potentiellement affecté par un incident, l'échange et la discussion portant sur les informations en rapport avec cet incident et les cybermenaces, risques et vulnérabilités connexes; g) à la demande d'un membre du réseau des CSIRT, la discussion et, si possible, la mise en œuvre d'une réponse coordonnée à un incident déterminé qui relève de la compétence de l'État membre concerné; h) la fourniture aux États membres d'une assistance face aux incidents transfrontières en application de la présente directive; i) la coopération, l'échange des meilleures pratiques et la fourniture d'une assistance aux CSIRT désignés comme coordinateurs conformément à l'article 12, paragraphe 1, en ce qui concerne la gestion de la divulgation coordonnée des vulnérabilités susceptibles d'avoir un impact important sur des entités de plusieurs États membres; j) la discussion et l'identification d'autres formes de coopération opérationnelle, notamment en rapport avec: i. les catégories de cybermenaces et d'incidents; ii. les alertes précoces;		

	iii. l'assistance mutuelle; iv. les principes et modalités d'une coordination en réponse à des risques et incidents transfrontières; v. la contribution au plan national de réaction aux crises et incidents de cybersécurité majeurs visé à l'article 9, paragraphe 4, à la demande d'un État membre; k) l'information du groupe de coopération de ses activités et des autres formes de coopération opérationnelle débattues en application du point j) et, lorsque cela s'avère nécessaire, la demande de fourniture d'orientations à cet égard; l) l'examen des exercices de cybersécurité, y compris ceux organisés par l'ENISA; m) à la demande d'un CSIRT donné, l'étude des capacités et de l'état de préparation dudit CSIRT; n) la coopération et l'échange d'informations avec les centres d'opérations de sécurité (SOC) régionaux et au niveau de l'Union afin d'améliorer la connaissance commune de la situation concernant les incidents et les cybermenaces dans toute l'Union;		

	o) s'il y a lieu, l'examen des rapports de l'évaluation par les pairs visés à l'article 19, paragraphe 9; p) la fourniture de lignes directrices afin de faciliter la convergence des pratiques opérationnelles en ce qui concerne l'application des dispositions du présent article relatives à la coopération opérationnelle.		
N/A	Art. 15, 4. Au plus tard le 17 janvier 2025, puis tous les deux ans, le réseau des CSIRT évalue, aux fins du réexamen visé à l'article 40, les progrès réalisés en matière de coopération opérationnelle et adopte un rapport. Le rapport formule notamment des conclusions et des recommandations à partir des résultats des évaluations par les pairs visées à l'article 19 et concernant les CSIRT nationaux. Ce rapport est aussi transmis au groupe de coopération.		
N/A	Art. 15, 5. Le réseau des CSIRT adopte son règlement intérieur.		
N/A	Art. 15, 6.		

	Le réseau des CSIRT et EU-CyCLONe fixent ensemble les modalités procédurales et coopèrent sur la base de ces modalités.		
N/A	Art. 16, 1. EU-CyCLONe est institué afin de contribuer à la gestion coordonnée, au niveau opérationnel, des incidents de cybersécurité majeurs et des crises, et de garantir l'échange régulier d'informations pertinentes entre les États membres et les institutions, organes et organismes de l'Union.		
N/A	Art. 16, 2. EU-CyCLONe est composé des représentants des autorités des États membres chargées de la gestion des crises de cybersécurité, ainsi que de la Commission lorsqu'un incident de cybersécurité majeur, potentiel ou en cours, a ou est susceptible d'avoir un impact important sur les services et les activités relevant du champ d'application de la présente directive. Dans les autres situations, la Commission participe aux activités d'EU-CyCLONe en qualité d'observateur. L'ENISA assure le secrétariat d'EU-CyCLONe et soutient l'échange sécurisé d'informations, et fournit également les outils nécessaires pour soutenir la coopération entre États membres en		

	garantissant un échange sécurisé d'informations. Si besoin est, EU-CyCLONe peut inviter des représentants des acteurs concernés à participer à ses travaux en qualité d'observateurs.		
N/A	Art. 16, 3. EU-CyCLONe a pour tâches: a) de renforcer le niveau de préparation à la gestion des incidents de cybersécurité majeurs et des crises; b) de développer une connaissance situationnelle partagée des incidents de cybersécurité majeurs et des crises; c) d'évaluer les conséquences et l'impact des incidents de cybersécurité majeurs et des crises en question et de proposer d'éventuelles mesures d'atténuation; d) de coordonner la gestion des incidents de		

	cybersécurité majeurs et des crises et de soutenir la prise de décision au niveau politique en ce qui concerne ces incidents et ces crises; e) d'examiner, à la demande de l'État membre concerné, le plan national de réaction aux crises et aux incidents de cybersécurité majeurs visé à l'article 9, paragraphe 4.		
N/A	Art. 16, 4. EU-CyCLONe adopte son règlement intérieur.		
N/A	Art. 16, 5. EU-CyCLONe rend régulièrement compte au groupe de coopération de la gestion des incidents de cybersécurité majeurs et des crises, ainsi que des tendances, en mettant notamment l'accent sur leur impact sur les entités essentielles et importantes.		
N/A	Art. 16, 6. EU-CyCLONe coopère avec le réseau des CSIRT sur la base des modalités procédurales convenues		

	conformément à l'article 15, paragraphe 6.		
N/A	Art. 16, 7. Au plus tard le 17 juillet 2024 et tous les 18 mois par la suite, EU-CyCLONe soumet au Parlement européen et au Conseil un rapport évaluant ses travaux.		
N/A	Art. 17. L'Union peut, conformément à l'article 218 du traité sur le fonctionnement de l'Union européenne et lorsque cela est pertinent, conclure avec des pays tiers ou des organisations internationales des accords internationaux qui permettent et organisent leur participation à certaines activités du groupe de coopération, du réseau des CSIRT et d'EU-CyCLONe. Ces accords sont conformes au droit de l'Union en matière de protection des données.		
N/A	Art. 18, 1. L'ENISA adopte, en coopération avec la Commission et le groupe de coopération, un rapport bisannuel sur l'état de la cybersécurité dans l'Union et le soumet et le présente au Parlement européen. Le rapport est notamment mis à disposition dans un format lisible par machine et		

	comporte les éléments suivants: a) une évaluation des risques en matière de cybersécurité à l'échelle de l'Union, qui tient compte du panorama des cybermenaces; b) une évaluation du développement des capacités de cybersécurité dans les secteurs public et privé dans l'ensemble de l'Union; c) une évaluation du degré général de sensibilisation à la cybersécurité et de cyberhygiène des citoyens et des entités, y compris les petites et moyennes entreprises; d) une évaluation agrégée du résultat des évaluations par les pairs visées à l'article 19; e) une évaluation agrégée du niveau de maturité des capacités de cybersécurité et des ressources en la matière dans l'ensemble de l'Union, notamment au niveau sectoriel, ainsi que du degré d'harmonisation des stratégies nationales en matière de cybersécurité des États membres.		
N/A	Art. 18, 2. Le rapport comprend des recommandations politiques spécifiques visant à remédier aux lacunes et à accroître le niveau de cybersécurité dans l'Union, ainsi qu'un résumé des conclusions pour la période concernée des rapports de situation		

	technique en matière de cybersécurité de l'Union européenne sur les incidents et cybermenaces, élaborés par l'ENISA conformément à l'article 7, paragraphe 6, du règlement (UE) 2019/881.		
N/A	Art. 18, 3. L'ENISA, en coopération avec la Commission, le groupe de coopération et le réseau des CSIRT, élabore la méthodologie, y compris les variables pertinentes, telles que les indicateurs quantitatifs et qualitatifs, de l'évaluation agrégée visée au paragraphe 1, point e).		
N/A	Art. 19, 1. Le groupe de coopération établit, au plus tard le 17 janvier 2025, avec l'aide de la Commission et de l'ENISA et, s'il y a lieu, du réseau des CSIRT, la méthodologie et les aspects organisationnels des évaluations par les pairs en vue de tirer des enseignements des expériences partagées, de renforcer la confiance mutuelle, de parvenir à un niveau élevé commun de cybersécurité, ainsi que de renforcer les capacités et les politiques des États membres en matière de cybersécurité qui sont nécessaires à la mise en œuvre de la présente directive. La participation aux évaluations par les pairs s'effectue à titre volontaire. Les évaluations par les pairs sont effectuées par des experts en		

	cybersécurité. Ces experts en cybersécurité sont désignés par au moins deux États membres différents de l'État membre faisant l'objet de l'évaluation. Les évaluations par les pairs portent au moins sur l'un des points suivants: a) le niveau de mise en œuvre des mesures de gestion des risques en matière de cybersécurité et des obligations d'information prévues aux articles 21 et 23; b) le niveau des capacités, y compris les ressources financières, techniques et humaines disponibles, et l'efficacité de l'exercice des tâches des autorités compétentes; c) les capacités opérationnelles des CSIRT; d) le niveau de mise en œuvre de l'assistance mutuelle visée à l'article 37; e) le niveau de mise en œuvre des accords de partage d'informations en matière de cybersécurité visés à l'article 29; f) des questions spécifiques de nature transfrontière ou transsectorielle.		
N/A	Art. 19, 2. La méthodologie visée au paragraphe 1 comprend des critères objectifs, non discriminatoires,		

	équitables et transparents sur la base desquels les États membres désignent les experts en cybersécurité habilités à effectuer les évaluations par les pairs. La Commission et l'ENISA participent en tant qu'observateurs aux évaluations par les pairs.		
N/A	Art. 19, 3. Les États membres peuvent définir des questions spécifiques visées au paragraphe 1, point f), aux fins d'une évaluation par les pairs.		
N/A	Art. 19, 4. Avant d'entamer l'évaluation par les pairs visée au paragraphe 1, les États membres en notifient la portée, en ce compris les questions définies en vertu du paragraphe 3, aux États membres qui y participent.		
N/A	Art. 19, 5. Avant le début de l'évaluation par les pairs, les États membres peuvent procéder à une autoévaluation des aspects évalués et fournir celle-ci aux experts en cybersécurité désignés. Le groupe de coopération établit, avec l'aide de la Commission et de l'ENISA, la méthode pour		

	l'autoévaluation des États membres.		
N/A	Art. 19, 6. Les évaluations par les pairs comportent des visites sur place physiques ou virtuelles et des échanges d'information hors site. Conformément au principe de bonne coopération, l'État membre faisant l'objet de l'évaluation par les pairs fournit aux experts en cybersécurité désignés les informations nécessaires à l'évaluation, sans préjudice du droit de l'Union ou du droit national concernant la protection des informations confidentielles ou classifiées, ni de la préservation des fonctions essentielles de l'État, telles que la sécurité nationale. Le groupe de coopération, en coopération avec la Commission et l'ENISA, élabore des codes de conduite appropriés qui sous-tendent les méthodes de travail des experts en cybersécurité désignés. Toute information obtenue durant l'évaluation par les pairs n'est utilisée qu'à cet effet. Les experts en cybersécurité participant à l'évaluation par les pairs ne divulguent à aucun tiers les informations sensibles ou confidentielles obtenues au cours de cette évaluation par les pairs.		
N/A	Art. 19, 7. Une fois qu'ils ont fait l'objet d'une évaluation par les pairs dans un État membre, les mêmes aspects		

	ne font pas l'objet d'une nouvelle évaluation par les pairs dans cet État membre au cours des deux années suivant la conclusion de l'évaluation par les pairs, sauf si l'État membre le demande ou si une proposition en ce sens du groupe de coopération est approuvée.		
N/A	Art. 19, 8. Les États membres veillent à ce que tout risque de conflit d'intérêts concernant les experts en cybersécurité désignés soit révélé aux autres États membres, au groupe de coopération, à la Commission et à l'ENISA, avant le début de l'évaluation par les pairs. L'État membre faisant l'objet de l'évaluation par les pairs peut s'opposer à la désignation de certains experts en cybersécurité pour des raisons dûment motivées communiquées à l'État membre qui les a désignés.		
N/A	Art. 19, 9. Les experts en cybersécurité participant aux évaluations par les pairs rédigent des rapports sur les résultats et les conclusions des évaluations par les pairs. Les États membres qui font l'objet d'une évaluation par les pairs peuvent formuler des observations sur les projets de rapport les concernant et ces observations sont jointes aux rapports. Les rapports contiennent des		

	recommandations permettant d'améliorer les aspects sur lesquels l'évaluation par les pairs a porté. Les rapports sont soumis, s'il y a lieu, au groupe de coopération et au réseau des CSIRT. Un État membre qui a fait l'objet d'une évaluation par les pairs peut décider de rendre public le rapport le concernant ou une version expurgée de celui-ci.		
Art. 14 Les entités essentielles, les entités importantes, les administrations de l'Etat et leurs établissements publics administratifs qui exercent leurs activités dans les domaines de la sécurité publique, de la défense et de la sécurité nationale ainsi que de la répression pénale, les missions diplomatiques et consulaires françaises pour leurs réseaux et systèmes d'information, le Commissariat à l'énergie atomique et aux énergies alternatives pour ses activités dans le domaine de la défense ainsi que les juridictions administratives et judiciaires prennent les mesures techniques, opérationnelles et organisationnelles appropriées et proportionnées pour gérer les risques qui menacent la sécurité des réseaux et des systèmes d'information qu'elles utilisent 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. Ces mesures garantissent, pour leurs réseaux et leurs systèmes d'information, un	<u>Art. 20, 1.</u> Les États membres veillent à ce que les organes de direction des entités essentielles et importantes approuvent les mesures de gestion des risques en matière de cybersécurité prises par ces entités afin de se conformer à l'article 21, supervisent sa mise en œuvre et puissent être tenus responsables de la violation dudit article par ces entités. L'application du présent paragraphe est sans préjudice du droit national en ce qui concerne les règles en matière de responsabilité applicables aux institutions publiques, ainsi que de responsabilité des agents de la fonction publique et des responsables élus ou nommés.	Norme de niveau législatif, qui sera à décliner par un décret.	Cf. Fiche d'impact « Périmètre de compétence de l'ANSSI et exigences de sécurité ». Les objectifs de sécurité prévus par voie réglementaire par l'article 14 prévoit la sensibilisation à cybersécurité et la mise en place d'une gouvernance par les risques sous la responsabilité du dirigeant exécutif de l'entité.

niveau de sécurité adapté et proportionné au risque existant. Elles visent à : 1° Mettre en place un pilotage de la sécurité des réseaux et systèmes d'information adaptée, comprenant notamment la formation à la cybersécurité des membres des organes de direction et des personnes exposées aux risques ; 2° Assurer la protection des réseaux et systèmes d'information, y compris en cas de recours à la sous-traitance ; 3° Mettre en place des outils et des procédures pour assurer la défense des réseaux et systèmes d'information et gérer les incidents ; 4° Garantir la résilience des activités. Un décret en Conseil d'Etat fixe les objectifs auxquels doivent se conformer les personnes mentionnées au premier alinéa afin que les mesures adoptées pour la gestion des risques satisfassent aux 1° à 4°. Ce décret détermine également les conditions d'élaboration, de modification et de publication d'un référentiel d'exigences techniques et organisationnelles qui sont adaptées aux différentes personnes mentionnées au premier alinéa.			
Art. 14 Les entités essentielles, les entités importantes, les administrations de l'Etat et leurs établissements	Art. 20, 2. Les États membres veillent à ce que les membres des organes de direction des entités essentielles et	Norme de niveau législatif, qui sera à	Cf. Fiche d'impact « Périmètre de compétence de l'ANSSI et exigences de

publics administratifs qui exercent leurs activités dans les domaines de la sécurité publique, de la défense et de la sécurité nationale ainsi que de la répression pénale, les missions diplomatiques et consulaires françaises pour leurs réseaux et systèmes d'information, le Commissariat à l'énergie atomique et aux énergies alternatives pour ses activités dans le domaine de la défense ainsi que les juridictions administratives et judiciaires prennent les mesures techniques, opérationnelles et organisationnelles appropriées et proportionnées pour gérer les risques qui menacent la sécurité des réseaux et des systèmes d'information qu'elles utilisent 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. Ces mesures garantissent, pour leurs réseaux et leurs systèmes d'information, un niveau de sécurité adapté et proportionné au risque existant. Elles visent à : 1° Mettre en place un pilotage de la sécurité des réseaux et systèmes d'information adaptée, comprenant notamment la formation à la cybersécurité des membres des organes de direction et des personnes exposées aux risques ; 2° Assurer la protection des réseaux et systèmes d'information, y compris en cas de recours à la sous-traitance ; 3° Mettre en place des outils et des procédures pour	importantes soient tenus de suivre une formation et ils encouragent les entités essentielles et importantes à offrir régulièrement une formation similaire aux membres de leur personnel afin que ceux-ci acquièrent des connaissances et des compétences suffisantes pour déterminer les risques et évaluer les pratiques de gestion des risques en matière de cybersécurité et leur impact sur les services fournis par l'entité.	décliner par un décret.	sécurité ». Les objectifs de sécurité prévus par voie réglementaire par l'article 14 prévoit la formation pour les personnels occupant des responsabilités dans le domaine du numérique (par exemple : directeur des systèmes d'information, responsable de la sécurité des systèmes d'information, administrateurs).

assurer la défense des réseaux et systèmes d'information et gérer les incidents ; 4° Garantir la résilience des activités. Un décret en Conseil d'Etat fixe les objectifs auxquels doivent se conformer les personnes mentionnées au premier alinéa afin que les mesures adoptées pour la gestion des risques satisfassent aux 1° à 4°. Ce décret détermine également les conditions d'élaboration, de modification et de publication d'un référentiel d'exigences techniques et organisationnelles qui sont adaptées aux différentes personnes mentionnées au premier alinéa.			
Art. 14 Les entités essentielles, les entités importantes, les administrations de l'Etat et leurs établissements publics administratifs qui exercent leurs activités dans les domaines de la sécurité publique, de la défense et de la sécurité nationale ainsi que de la répression pénale, les missions diplomatiques et consulaires françaises pour leurs réseaux et systèmes d'information, le Commissariat à l'énergie atomique et aux énergies alternatives pour ses activités dans le domaine de la défense ainsi que les juridictions administratives et judiciaires prennent les mesures techniques, opérationnelles et organisationnelles appropriées et proportionnées pour gérer les risques qui menacent la sécurité des réseaux et des systèmes d'information qu'elles utilisent dans le cadre de leurs	<u>Art. 21, 1.</u> Les États membres veillent à ce que les entités essentielles et importantes prennent les mesures techniques, opérationnelles et organisationnelles appropriées et proportionnées pour gérer les risques qui menacent la sécurité des réseaux et des systèmes d'information que ces entités utilisent dans le cadre de leurs activités ou de la fourniture de leurs services, ainsi que pour éliminer ou réduire les conséquences que les incidents ont sur les destinataires de leurs services et sur d'autres services. Les mesures visées au premier alinéa garantissent, pour les réseaux et les systèmes d'information, un	Norme de niveau législatif, qui sera à décliner par un décret.	Cf. Fiche d'impact « Périmètre de compétence de l'ANSSI et exigences de sécurité ».

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. Ces mesures garantissent, pour leurs réseaux et leurs systèmes d'information, un niveau de sécurité adapté et proportionné au risque existant. Elles visent à : 1° Mettre en place un pilotage de la sécurité des réseaux et systèmes d'information adaptée, comprenant notamment la formation à la cybersécurité des membres des organes de direction et des personnes exposées aux risques ; 2° Assurer la protection des réseaux et systèmes d'information, y compris en cas de recours à la sous-traitance ; 3° Mettre en place des outils et des procédures pour assurer la défense des réseaux et systèmes d'information et gérer les incidents ; 4° Garantir la résilience des activités. Un décret en Conseil d'Etat fixe les objectifs auxquels doivent se conformer les personnes mentionnées au premier alinéa afin que les mesures adoptées pour la gestion des risques satisfassent aux 1° à 4°. Ce décret détermine également les conditions d'élaboration, de modification et de publication d'un référentiel d'exigences techniques et organisationnelles qui sont adaptées aux différentes personnes mentionnées au	niveau de sécurité adapté au risque existant, en tenant compte de l'état des connaissances et, s'il y a lieu, des normes européennes et internationales applicables, ainsi que du coût de mise en œuvre. Lors de l'évaluation de la proportionnalité de ces mesures, il convient de tenir dûment compte du degré d'exposition de l'entité aux risques, de la taille de l'entité et de la probabilité de survenance d'incidents et de leur gravité, y compris leurs conséquences sociétales et économiques.		

premier alinéa.			
Art. 14 Un décret en Conseil d'Etat fixe les objectifs auxquels doivent se conformer les personnes mentionnées au premier alinéa afin que les mesures adoptées pour la gestion des risques satisfassent aux 1° à 4°. Ce décret détermine également les conditions d'élaboration, de modification et de publication d'un référentiel d'exigences techniques et organisationnelles qui sont adaptées aux différentes personnes mentionnées au premier alinéa.	<u>Art. 21, 2.</u> Les mesures visées au paragraphe 1 sont fondées sur une approche «tous risques» qui vise à protéger les réseaux et les systèmes d'information ainsi que leur environnement physique contre les incidents, et elles comprennent au moins: a) les politiques relatives à l'analyse des risques et à la sécurité des systèmes d'information ; b) la gestion des incidents; c) la continuité des activités, par exemple la gestion des sauvegardes et la reprise des activités, et la gestion des crises; d) 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; e) 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; f) des politiques et des procédures pour	Norme de niveau législatif, qui sera à décliner par un décret.	Cf. Fiche d'impact « Périmètre de compétence de l'ANSSI et exigences de sécurité ». Le modèle choisi par la France pour répondre à ce principe consiste à définir au niveau réglementaire des objectifs de sécurité définis en cohérence avec les points a) à j) du 2. de l'article 21. Pour atteindre ces objectifs, l'autorité nationale de sécurité des systèmes d'information élabore un référentiel de cybersécurité sur lequel les entités importantes ou essentielles peuvent s'appuyer et s'en prévaloir auprès de l'autorité nationale de sécurité des systèmes

	évaluer l'efficacité des mesures de gestion des risques en matière de cybersécurité; g) les pratiques de base en matière de cyberhygiène et la formation à la cybersécurité; h) des politiques et des procédures relatives à l'utilisation de la cryptographie et, le cas échéant, du chiffrement; i) la sécurité des ressources humaines, des politiques de contrôle d'accès et la gestion des actifs; j) 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.		d'information lors des contrôles.
N/A	Art. 21, 3. Les États membres veillent à ce que, lorsqu'elles examinent lesquelles des mesures visées au paragraphe 2, point d), du présent article sont appropriées, les entités tiennent compte des vulnérabilités propres à chaque fournisseur et prestataire de services direct et de la qualité globale des produits et des pratiques de cybersécurité de leurs fournisseurs et prestataires de services, y compris de leurs procédures de développement sécurisé. Les États membres veillent également à		

	ce que, lorsqu'elles examinent lesquelles des mesures visées audit point sont appropriées, les entités soient tenues de prendre en compte les résultats des évaluations coordonnées des risques pour la sécurité des chaînes d'approvisionnement critiques, effectuées conformément à l'article 22, paragraphe 1.		
N/A	Art. 21, 4. Les États membres veillent à ce que, lorsqu'une entité constate qu'elle ne se conforme pas aux mesures prévues au paragraphe 2, elle prenne, sans retard injustifié, toutes les mesures correctives nécessaires appropriées et proportionnées.		
Art. 14 Par dérogation aux deux alinéas précédents, les fournisseurs de services de systèmes de noms de domaine, les offices d'enregistrement, les fournisseurs de services d'informatique en nuage, les fournisseurs de services de centres de données, les fournisseurs de réseaux de diffusion de contenu, les fournisseurs de services gérés, les fournisseurs de 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 mettent en œuvre les exigences techniques et méthodologiques qui leur	Art. 21, 5. Au plus tard le 17 octobre 2024, la Commission adopte des actes d'exécution établissant les exigences techniques et méthodologiques liées aux mesures visées au paragraphe 2 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		

sont propres.	moteurs de recherche en ligne et de plateformes de services de réseaux sociaux, et les prestataires de services de confiance. La Commission peut adopter des actes d'exécution établissant les exigences techniques et méthodologiques ainsi que les exigences sectorielles, si nécessaire, liées aux mesures visées au paragraphe 2 concernant les entités essentielles et importantes autres que celles visées au premier alinéa du présent paragraphe. Lorsqu'elle prépare les actes d'exécution visés aux premier et deuxième alinéas du présent paragraphe, la Commission suit, dans la mesure du possible, les normes européennes et internationales ainsi que les spécifications techniques pertinentes. La Commission échange des conseils et coopère avec le groupe de coopération et l'ENISA sur les projets d'actes d'exécution conformément à l'article 14, paragraphe 4, point e). Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 39, paragraphe 2.		
N/A	Art. 22, 1. Le groupe de coopération, en coopération avec la Commission et l'ENISA, peut procéder à des		

	évaluations coordonnées des risques pour la sécurité des chaînes d'approvisionnement de services TIC, de systèmes TIC ou de produits TIC critiques spécifiques, en tenant compte des facteurs de risque techniques et, le cas échéant, non techniques.		
N/A	Art. 22, 2. La Commission, après avoir consulté le groupe de coopération et l'ENISA et, selon le cas, les acteurs concernés, détermine les services TIC, systèmes TIC ou produits TIC critiques spécifiques qui peuvent faire l'objet de l'évaluation coordonnée des risques de sécurité visée au paragraphe 1.		
Art. 17, premier et dernier alinéa Les personnes mentionnées à l'article 14 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. Un décret en Conseil d'Etat 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 ainsi que les délais de notification des incidents et des vulnérabilités	Art. 23, 1. Chaque État membre veille à ce que les entités essentielles et importantes notifient, sans retard injustifié, à son CSIRT ou, selon le cas, à son autorité compétente, conformément au paragraphe 4, tout incident ayant un impact important sur leur fourniture des services visés au paragraphe 3 (ci-après dénommé «incident important»). Le cas échéant, les entités concernées notifient, sans retard injustifié, aux destinataires de leurs services les incidents importants susceptibles de nuire à la fourniture de ces services. Chaque État membre veille à ce que ces entités signalent, entre autres,	Norme de niveau législatif, qui sera à décliner par un décret.	Cf. Fiche d'impact « Notification d'incidents et partage d'informations ». Les modalités liées : 1) aux critères de qualification d'un incident important, 2) à la procédure de notification des

	toute information permettant au CSIRT ou, le cas échéant, à l'autorité compétente de déterminer si l'incident a un impact transfrontière. Le simple fait de notifier un incident n'accroît pas la responsabilité de l'entité qui est à l'origine de la notification. Lorsque les entités concernées notifient un incident important à l'autorité compétente en application du premier alinéa, l'État membre veille à ce que cette autorité compétente transmette la notification au CSIRT dès qu'elle la reçoit. En cas d'incident important transfrontière ou transsectoriel, les États membres veillent à ce que leurs points de contact uniques reçoivent en temps utile les informations notifiées conformément au paragraphe 4.		incidents de sécurité, 3) aux informations à notifier à l'autorité nationale de sécurité des systèmes d'information sont définies au niveau réglementaire Le modèle français de transposition de la directive devrait prévoir, au niveau règlementaire, que les rôles d'autorité compétente, de CSIRT et de point de contact unique soient assumés par l'autorité nationale de sécurité des systèmes d'information (sauf pour certaines activités dans le domaine de la défense). Les dispositions du 2ème et 3ème alinéa sont *de facto*

			pris en compte.
Art. 17, troisième alinéa Les entités essentielles et importantes notifient sans délai aux destinataires de leurs services : 1° Les incidents critiques susceptibles de nuire à la fourniture de ces services ; 2° 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.	Art. 23, 2. Le cas échéant, les États membres veillent à ce que les entités essentielles et importantes communiquent, sans retard injustifié, aux destinataires de leurs services qui sont potentiellement affectés par une cybermenace importante toutes les mesures ou corrections que ces destinataires peuvent appliquer en réponse à cette menace. Le cas échéant, les entités informent également ces destinataires de la cybermenace importante elle-même.		Cf. Fiche d'impact « Notification d'incidents et partage d'informations ».
N/A	Art. 23, 3. Un incident est considéré comme important si: a) il a causé ou est susceptible de causer une perturbation opérationnelle grave des services ou des pertes financières pour l'entité concernée; b) il a affecté ou est susceptible d'affecter d'autres personnes physiques ou morales en causant des dommages matériels, corporels ou moraux considérables.		Les modalités liées : 1) aux critères de qualification d'un incident important, 2) à la procédure de notification des incidents de sécurité, 3) aux informations à notifier à l'autorité nationale de

			sécurité des systèmes d'information sont définies au niveau réglementaire
N/A	<u>Art. 23, 4.</u> Les États membres veillent à ce que, aux fins de la notification visée au paragraphe 1, les entités concernées soumettent au CSIRT ou, selon le cas, à l'autorité compétente: a) sans retard injustifié et en tout état de cause dans les 24 heures après avoir eu connaissance de l'incident important, une alerte précoce qui, le cas échéant, indique si l'on suspecte l'incident important d'avoir été causé par des actes illicites ou malveillants ou s'il pourrait avoir un impact transfrontière; b) sans retard injustifié et en tout état de cause dans les 72 heures après avoir eu connaissance de l'incident important, une notification d'incident qui, le cas échéant, met à jour les informations visées au point a) et 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;		Les modalités liées : 1) aux critères de qualification d'un incident important, 2) à la procédure de notification des incidents de sécurité, 3) aux informations à notifier à l'autorité nationale de sécurité des systèmes d'information sont définies au niveau réglementaire

	c) à la demande d'un CSIRT ou, selon le cas, de l'autorité compétente, un rapport intermédiaire sur les mises à jour pertinentes de la situation; d) un rapport final au plus tard un mois après la présentation de la notification d'incident visée au point b), comprenant les éléments suivants: i. une description détaillée de l'incident, y compris de sa gravité et de son impact; ii. le type de menace ou la cause profonde qui a probablement déclenché l'incident; iii. les mesures d'atténuation appliquées et en cours; iv. le cas échéant, l'impact transfrontière de l'incident; e) en cas d'incident en cours au moment de la présentation du rapport final visé au point d), les États membres veillent à ce que les entités concernées fournissent à ce moment-là un rapport d'avancement puis un rapport final dans un délai d'un mois à compter du traitement de l'incident. Par dérogation au premier alinéa, point b), un prestataire de services de confiance notifie au CSIRT ou, selon le cas, à l'autorité compétente les incidents importants qui ont un impact sur la		

	fourniture de ses services de confiance, sans retard injustifié et en tout état de cause dans les 24 heures après avoir eu connaissance de l'incident important.		
N/A	Art. 23, 5. Le CSIRT ou l'autorité compétente fournissent, sans retard injustifié et si possible dans les 24 heures suivant la réception de l'alerte précoce visée au paragraphe 4, point a), 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. Lorsque le CSIRT n'est pas le premier destinataire de la notification visée au paragraphe 1, l'orientation est émise par l'autorité compétente en coopération avec le CSIRT. Le CSIRT fournit un soutien technique supplémentaire si l'entité concernée le demande. Lorsqu'il y a lieu de suspecter que l'incident est de nature criminelle, le CSIRT ou l'autorité compétente fournit également des orientations sur les modalités de notification de l'incident important aux autorités répressives.		Les modalités liées : 1) aux critères de qualification d'un incident important, 2) à la procédure de notification des incidents de sécurité, 3) aux informations à notifier à l'autorité nationale de sécurité des systèmes d'information sont définies au niveau réglementaire
Art. 23 Les dispositions de l'article 11 du code de procédure	Art. 23, 6. Lorsque c'est approprié, et notamment si l'incident	Norme de niveau	Cf. Fiche d'impact « Notification

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'autorité nationale de sécurité des systèmes d'information, et, d'autre part, la Commission nationale de l'informatique et des libertés 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 Etats membres de l'Union européenne ou des centres de réponse aux incidents de sécurité informatique ou des organismes internationaux concourant aux missions de sécurité ou de défense des systèmes d'information. Les modalités d'application du présent article, notamment les modalités du partage d'informations, sont déterminées par décret en Conseil d'Etat.	important concerne deux États membres ou plus, le CSIRT, l'autorité compétente ou le point de contact unique informent sans retard injustifié les autres États membres touchés et l'ENISA de l'incident important. Sont alors partagées des informations du type de celles reçues conformément au paragraphe 4. Ce faisant, le CSIRT, l'autorité compétente ou le point de contact unique doivent, dans le respect du droit de l'Union ou du droit national, préserver la sécurité et les intérêts commerciaux de l'entité ainsi que la confidentialité des informations communiquées.	législatif, qui sera à décliner par un décret.	d'incidents et partage d'informations ».
Art. 17, second alinéa Pour prévenir un incident concernant une entité essentielle ou une entité importante ou pour faire face à un incident en cours ou lorsque la divulgation de	Art. 23, 7. Lorsque la sensibilisation du public est nécessaire pour prévenir un incident important ou pour faire face à un incident important en cours, ou lorsque la		Cf. Fiche d'impact « Notification d'incidents et partage d'informations ».

l'incident est dans l'intérêt public, l'autorité nationale de sécurité des systèmes d'information peut, après avoir consulté l'entité essentielle ou importante concernée, exiger de celle-ci qu'elle informe le public de l'incident ou le faire elle-même.	divulgation de l'incident important est par ailleurs dans l'intérêt public, le CSIRT d'un État membre ou, selon le cas, son autorité compétente et, le cas échéant, les CSIRT ou les autorités compétentes des autres États membres concernés peuvent, après avoir consulté l'entité concernée, informer le public de l'incident important ou exiger de l'entité qu'elle le fasse.		
Art. 23 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'autorité nationale de sécurité des systèmes d'information, et, d'autre part, la Commission nationale de l'informatique et des libertés 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 Etats membres de l'Union européenne ou des centres de réponse aux incidents de sécurité	<u>Art. 23, 8.</u> À la demande du CSIRT ou de l'autorité compétente, le point de contact unique transmet les notifications reçues en vertu du paragraphe 1 aux points de contact uniques des autres États membres touchés.	Norme de niveau législatif, qui sera à décliner par un décret.	Cf. Fiche d'impact « Notification d'incidents et partage d'informations ». L'article 23 prévoit un cadre de coopération pour l'autorité nationale de sécurité des systèmes d'information qui assure les rôles d'autorité compétente, de CSIRT et de point de contact unique, sauf pour certaines activités dans le domaine de la défense où d'autres organismes pourront exercer ces missions sur désignation du Premier ministre.

informatique ou des organismes internationaux concourant aux missions de sécurité ou de défense des systèmes d'information. Les modalités d'application du présent article, notamment les modalités du partage d'informations, sont déterminées par décret en Conseil d'Etat.			
N/A	Art. 23, 9. Le point de contact unique soumet tous les trois mois à l'ENISA un rapport de synthèse comprenant des données anonymisées et agrégées sur les incidents importants, les incidents, les cybermenaces et les incidents évités notifiés conformément au paragraphe 1 du présent article et à l'article 30. Afin de contribuer à la fourniture d'informations comparables, l'ENISA peut adopter des orientations techniques sur les paramètres des informations à inclure dans le rapport de synthèse. L'ENISA informe le groupe de coopération et le réseau des CSIRT de ses conclusions concernant les notifications reçues tous les six mois.		
N/A	Art. 23, 10. Les CSIRT ou, selon le cas, les autorités compétentes fournissent aux autorités compétentes en vertu de la directive (UE) 2022/2557 des informations sur les incidents importants, les incidents, les cybermenaces et les incidents évités		Selon l'article R. 2321-1 du code de la défense, l'agence nationale de sécurité des systèmes d'information et l'autorité nationale de

	notifiés conformément au paragraphe 1 du présent article et à l'article 30 par les entités identifiées comme des entités critiques en vertu de la directive (UE) 2022/2557.		sécurité des systèmes d'information. Par ailleurs, l'agence nationale de sécurité des systèmes d'information est une direction du SGDSN qui est l'autorité compétente en vertu de la directive (UE) 2022/2557. L'organisation des services du SGDSN en termes de partage d'information relève du niveau règlementaire
N/A	Art. 23, 11. La Commission peut adopter des actes d'exécution précisant plus en détail le type d'informations, le format et la procédure des notifications présentées en vertu du paragraphe 1 du présent article et de l'article 30 ainsi que des communications présentées en vertu du paragraphe 2 du présent article. Au plus tard le 17 octobre 2024, la Commission adopte, 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, des actes d'exécution précisant plus en détail les cas dans lesquels un incident est considéré comme important au sens du paragraphe 3. La Commission peut adopter de tels actes d'exécution pour d'autres entités essentielles et importantes. La Commission échange des conseils et coopère avec le groupe de coopération sur les projets d'actes d'exécution visés aux premier et deuxième alinéas du présent paragraphe conformément à l'article 14, paragraphe 4, point e). Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 39, paragraphe 2.		
Art. 14, troisième alinéa Ce référentiel peut prescrire le recours à des produits, des services ou des processus certifiés au titre du	<u>Art. 24, 1.</u> Afin de démontrer la conformité à certaines exigences visées à l'article 21, les États membres	Norme de niveau législatif, qui sera à	Cf. Fiche d'impact « Périmètre de compétence de l'autorité nationale et exigences

règlement (UE) n° 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) no 526/2013.	peuvent prescrire aux entités essentielles et importantes d'utiliser des produits TIC, services TIC et processus TIC particuliers qui, mis au point par l'entité essentielle ou importante ou acquis auprès de tiers, sont certifiés dans le cadre de schémas européens de certification de cybersécurité adoptés conformément à l'article 49 du règlement (UE) 2019/881. En outre, les États membres encouragent les entités essentielles et importantes à utiliser des services de confiance qualifiés.	décliner par un décret.	de sécurité ». Les mesures visées à cet alinéa sont définies au niveau réglementaire.
N/A	Art. 24, 2. La Commission est habilitée à adopter des actes délégués, conformément à l'article 38, pour compléter la présente directive en précisant quelles catégories d'entités essentielles et importantes sont tenues d'utiliser certains produits TIC, services TIC et processus TIC certifiés ou d'obtenir un certificat dans le cadre d'un schéma européen de certification de cybersécurité adopté conformément à l'article 49 du règlement (UE) 2019/881. Ces actes délégués sont adoptés lorsque des niveaux insuffisants de cybersécurité ont été constatés et ils prévoient une période de mise en œuvre. Avant d'adopter de tels actes délégués, la Commission procède à une analyse d'impact et mène des consultations conformément à l'article 56		

	du règlement (UE) 2019/881.		
N/A	Art. 24, 3. Lorsqu'il n'existe pas de schéma européen de certification de cybersécurité approprié aux fins du paragraphe 2 du présent article, la Commission peut, après consultation du groupe de coopération et du groupe européen de certification de cybersécurité, demander à l'ENISA de préparer un schéma candidat conformément à l'article 48, paragraphe 2, du règlement (UE) 2019/881.		
N/A	Art. 25, 1. Afin de favoriser la mise en œuvre convergente de l'article 21, paragraphes 1 et 2, les États membres encouragent, sans imposer l'utilisation d'un type particulier de technologies ni créer de discrimination en faveur d'un tel type particulier de technologies, le recours à des normes et des spécifications techniques européennes et internationales pour la sécurité des réseaux et des systèmes d'information.		Ces recommandations sont prévues au niveau réglementaire dans le décret prévu par l'article 11 sur la définition des objectifs de sécurité que devront appliquer les entités importantes ou essentielles
N/A	Art. 25, 2. L'ENISA, en coopération avec les États membres et, le cas échéant, après consultation des acteurs		

	concernés, formule des avis et des lignes directrices concernant les domaines techniques qui doivent être pris en considération en lien avec le paragraphe 1 et concernant les normes existantes, y compris les normes nationales, qui permettraient de couvrir ces domaines.		
Art. 11, I. I. – Les entités essentielles et les entités importantes sont régies par les dispositions du présent titre lorsque, selon le cas : 1° Elles sont établies sur le territoire national ; 2° S'agissant des opérateurs de communications électroniques, ils fournissent leurs services sur le territoire national ; 3° S'agissant des fournisseurs de services de système de noms de domaine, des offices d'enregistrement, des fournisseurs de services d'informatique en nuage, des fournisseurs de services de centres de données, des fournisseurs de réseaux de diffusion de contenu, des fournisseurs de services gérés, des fournisseurs de services de sécurité gérés, ainsi que des fournisseurs de places de marché en ligne, de moteurs de recherche en ligne ou de plateformes de services de réseaux sociaux : a) Ils ont leur établissement principal sur le	<u>Art. 26, 1.</u> Les entités relevant du champ d'application de la présente directive sont considérées comme relevant de la compétence de l'État membre dans lequel elles sont établies, à l'exception des cas suivants: a) les fournisseurs de réseaux 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) les fournisseurs de services DNS, les registres des noms de domaine de premier niveau, les entités fournissant des services d'enregistrement de noms de domaine, les fournisseurs de services d'informatique en nuage, les fournisseurs de services de centres de données, les fournisseurs de réseaux de diffusion de contenu, les fournisseurs de services gérés,		Cf. Fiche d'impact « Périmètre de compétence de l'autorité nationale et exigences de sécurité ».

territoire national ; b) Ou, s'ils sont établis hors de l'Union européenne mais offrent leurs services sur le territoire national, ils ont désigné un représentant établi sur le territoire national. Toutefois, les conditions d'établissement sur le territoire national ne s'appliquent pas aux administrations et établissements publics.	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 en application du paragraphe 2; c) les entités de l'administration publique, qui sont considérées comme relevant de la compétence de l'État membre qui les a établies.		
N/A	<u>Art. 26, 2.</u> Aux fins de la présente directive, un entité visée au paragraphe 1, point b), est considérée avoir son établissement principal dans l'Union dans l'État membre où sont principalement prises les décisions relatives aux mesures de gestion des risques en matière de cybersécurité. Si un tel État membre ne peut être déterminé ou si ces décisions ne sont pas prises dans l'Union, l'établissement principal est considéré comme se trouvant dans l'État membre où les opérations de cybersécurité sont effectuées. Si un tel État membre ne peut être déterminé, l'établissement principal est considéré comme se trouvant dans l'État membre où l'entité concernée possède l'établissement comptant le plus grand nombre de salariés dans l'Union.		

N/A	Art. 26, 3. Si une entité visée au paragraphe 1, point b), n'est pas établie dans l'Union mais offre des services dans l'Union, elle désigne un représentant dans l'Union. Le représentant est établi dans l'un des États membres dans lesquels les services sont fournis. Une telle entité est considérée comme relevant de la compétence de l'État membre dans lequel le représentant est établi. En l'absence d'un représentant dans l'Union désigné en vertu du présent paragraphe, tout État membre dans lequel l'entité fournit des services peut intenter une action en justice contre l'entité pour violation de la présente directive.		
N/A	Art. 26, 4. La désignation d'un représentant par une entité visée au paragraphe 1, point b), est sans préjudice d'actions en justice qui pourraient être intentées contre l'entité elle-même.		
N/A	Art. 26, 5. Les États membres qui ont reçu une demande d'assistance mutuelle en lien avec une entité visée au paragraphe 1, point b), peuvent, dans les limites de cette demande, prendre des mesures de		Cf. Fiche d'impact « Missions et compétences de l'autorité nationale ».

	supervision et d'exécution appropriées à l'égard de l'entité concernée qui fournit des services ou qui dispose d'un réseau et d'un système d'information sur leur territoire.		
N/A	Art. 27, 1. L'ENISA crée et tient, sur la base des informations reçues des points de contact uniques conformément au paragraphe 4, un registre des fournisseurs de services DNS, des registres des noms de domaine de premier niveau, des entités qui fournissent des services d'enregistrement de noms de domaine, des fournisseurs de services d'informatique en nuage, des fournisseurs de services de centres de données, des fournisseurs de réseaux de diffusion de contenu, des fournisseurs de services gérés, des fournisseurs de services de sécurité gérés, ainsi que des fournisseurs de places de marché en ligne, de moteurs de recherche en ligne et de plateformes de services de réseaux sociaux. Sur demande, l'ENISA permet aux autorités compétentes d'accéder à ce registre, tout en veillant à ce que la confidentialité des informations soit protégée, s'il y a lieu.		
Art. 12 L'autorité nationale de sécurité des systèmes d'information établit et met à jour la liste des entités	Art. 27, 2. Les États membres demandent aux entités visées au paragraphe 1 de soumettre les informations	Norme de niveau législatif, qui	Cf. Fiche d'impact « Périmètre de compétence de l'ANSSI

essentielles, des entités importantes et des bureaux d'enregistrement sur la base des informations que ces entités et bureaux d'enregistrement lui communiquent. Les informations à transmettre, leurs modalités de communication et les délais dans lesquels les modifications doivent être transmises sont définis par décret en Conseil d'Etat.	suivantes aux autorités compétentes au plus tard le 17 janvier 2025: a) le nom de l'entité; b) les secteur, sous-secteur et type d'entité concernés, visés à l'annexe I ou II, le cas échéant; c) l'adresse de l'établissement principal de l'entité et de ses autres établissements légaux dans l'Union ou, si elle n'est pas établie dans l'Union, de son représentant désigné conformément à l'article 26, paragraphe 3; d) les coordonnées actualisées, y compris les adresses de courrier électronique et les numéros de téléphone de l'entité et, le cas échéant, de son représentant désigné conformément à l'article 26, paragraphe 3; e) les États membres dans lesquels l'entité fournit des services; et f) les plages d'IP de l'entité.	sera à décliner par un décret.	et exigences de sécurité ».
Art. 12 L'autorité nationale de sécurité des systèmes d'information établit et met à jour la liste des entités essentielles, des entités importantes et des bureaux d'enregistrement sur la base des informations que ces entités et bureaux d'enregistrement lui communiquent. Les informations à transmettre, leurs modalités de	<u>Art. 27, 3.</u> Les États membres veillent à ce que les entités visées au paragraphe 1 notifient à l'autorité compétente toute modification des informations qu'elles ont communiquées en vertu du paragraphe 2 sans tarder et, en tout état de cause, dans un délai de trois mois à compter de la date de la	Norme de niveau législatif, qui sera à décliner par un décret.	Cf. Fiche d'impact « Périmètre de compétence de l'ANSSI et exigences de sécurité ». Les délais de communication des

communication et les délais dans lesquels les modifications doivent être transmises sont définis par décret en Conseil d'Etat.	modification.		informations à l'autorité nationale de sécurité des systèmes d'information seront définis au niveau réglementaire
N/A	Art. 27, 4. À la réception des informations visées aux paragraphes 2 et 3, à l'exception des informations visées au paragraphe 2, point f), le point de contact unique de l'État membre concerné les transmet sans retard injustifié à l'ENISA.		
N/A	Art. 27, 5. S'il y a lieu, les informations visées aux paragraphes 2 et 3 du présent article sont communiquées via le mécanisme national visé à l'article 3, paragraphe 4, quatrième alinéa.		
Art. 19, premier et deuxième alinéa 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. Les offices et les bureaux d'enregistrement sont	Art. 28, 1. Afin de contribuer à la sécurité, à la stabilité et à la résilience du 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	Norme de niveau législatif, qui sera à décliner par un décret.	Cf. Fiche d'impact « Enregistrement des noms de domaine ».

responsables du traitement de ces données au regard de la réglementation en matière de protection des données personnelles. Ils tiennent ces bases de données à jour, en maintenant les données exactes et complètes, sans redondance de collecte. A cette fin, ils 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.	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.		
Art. 19, dernier alinéa Un décret en Conseil d'Etat, pris après avis de la Commission nationale informatique et libertés, fixe la liste des données relatives aux noms de domaine devant être collectées.	Art. 28, 2. Aux fins du paragraphe 1, 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: a) le nom de domaine; b) la date d'enregistrement; c) le nom du titulaire, l'adresse de courrier électronique et le numéro de téléphone permettant de le contacter; d) l'adresse de courrier électronique et le numéro de téléphone permettant de contacter le point de contact qui gère le nom de domaine, si ces coordonnées sont différentes de celles du	Norme de niveau législatif, qui sera à décliner par un décret.	Cf. Fiche d'impact « Enregistrement des noms de domaine ».

	titulaire.		
Art. 19, second alinéa Les offices et les bureaux d'enregistrement sont responsables du traitement de ces données au regard de la réglementation en matière de protection des données personnelles. Ils tiennent ces bases de données à jour, en maintenant les données exactes et complètes, sans redondance de collecte. A cette fin, ils 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.	Art. 28, 3. Les États membres exigent que les registres des noms de domaine de premier niveau et les entités fournissant des services d'enregistrement de noms de domaine aient mis en place des politiques et des procédures, notamment des procédures de vérification, visant à garantir que les bases de données 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.	Norme de niveau législatif, qui sera à décliner par un décret.	Cf. Fiche d'impact « Enregistrement des noms de domaine ».
Art. 21 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.	Art. 28, 4. Les États membres exigent que les registres des noms de domaine de premier niveau et les entités fournissant des services d'enregistrement de noms de domaine rendent publiques, sans retard injustifié après l'enregistrement d'un nom de domaine, les données d'enregistrement du nom de domaine qui ne sont pas des données à caractère personnel.		Cf. Fiche d'impact « Enregistrement des noms de domaine ».
Art. 22 Pour les besoins des procédures pénales et de la sécurité des systèmes d'information, les agents habilités à cet effet par l'autorité judiciaire ou par l'autorité nationale de sécurité des systèmes	Art. 28, 5. Les États membres imposent aux registres des noms de domaine de premier niveau et aux entités fournissant des services d'enregistrement de noms	Norme de niveau législatif, qui sera à décliner par	Cf. Fiche d'impact « Enregistrement des noms de domaine ».

d'information peuvent obtenir des offices et bureaux d'enregistrement les données mentionnées à l'article 20. Les offices et les bureaux d'enregistrement fixent les règles de procédure pour la communication de ces données aux agents mentionnés au premier alinéa. Cette communication intervient dans un délai n'excédant pas soixante-douze heures. Ces règles sont accessibles au public. Un décret en Conseil d'Etat, pris après avis de la Commission nationale de l'informatique et des libertés, fixe les modalités d'application du présent article.	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. 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. Les États membres imposent que les politiques et procédures de divulgation de ces données soient rendues publiques.	un décret.	
N/A	Art. 28, 6. Le respect des obligations énoncées aux paragraphes 1 à 5 ne saurait entraîner de répétition inutile de la collecte des données d'enregistrement de noms de domaine. À cet effet, les États membres imposent aux registres des noms de domaine de premier niveau et aux entités fournissant des services d'enregistrement de noms de domaine de coopérer entre eux.		
N/A	Art. 29, 1. Les États membres veillent à ce que les entités relevant du champ d'application de la présente		

	directive et, le cas échéant, les autres entités concernées ne relevant pas du champ d'application de la présente directive puissent échanger entre elles, à titre volontaire, des informations pertinentes en matière de cybersécurité, y compris des informations relatives aux cybermenaces, aux incidents évités, aux vulnérabilités, aux techniques et procédures, aux indicateurs de compromission, aux tactiques adverses, ainsi que des informations spécifiques sur les acteurs de la menace, des alertes de cybersécurité et des recommandations concernant la configuration des outils de cybersécurité pour détecter les cyberattaques, lorsque ce partage d'informations: a) vise à prévenir et à détecter les incidents, à y réagir, à s'en rétablir ou à atténuer leur impact; b) renforce le niveau de cybersécurité, notamment en sensibilisant aux cybermenaces, en limitant ou en empêchant leur capacité de se propager, en soutenant une série de capacités de défense, en remédiant aux vulnérabilités et en les révélant, en mettant en œuvre des techniques de détection, d'endiguement et de prévention des menaces, des stratégies d'atténuation ou des étapes de réaction et de rétablissement, ou en encourageant la recherche collaborative en matière de cybermenaces entre les entités publiques et privées.		

N/A	Art. 29, 2. Les États membres veillent à ce que l'échange d'informations ait lieu au sein de communautés d'entités essentielles et importantes ainsi que, le cas échéant, de leurs fournisseurs ou prestataires de services. Cet échange est mis en œuvre au moyen d'accords de partage d'informations en matière de cybersécurité, compte tenu de la nature potentiellement sensible des informations partagées.		
N/A	Art. 29, 3. Les États membres facilitent la mise en place des accords de partage d'informations en matière de cybersécurité visés au paragraphe 2 du présent article. Ces accords peuvent préciser les éléments opérationnels, y compris l'utilisation de plateformes TIC spécialisées et d'outils d'automatisation, le contenu et les conditions des accords de partage d'informations. Lorsqu'ils précisent la participation des autorités publiques à ces accords, les États membres peuvent imposer des conditions en ce qui concerne les informations mises à disposition par les autorités compétentes ou les CSIRT. Les États membres offrent un soutien à l'application de ces accords conformément à leurs politiques visées à l'article 7, paragraphe 2, point		

	h).		
N/A	Art. 29, 4. Les États membres veillent à ce que les entités essentielles et importantes notifient aux autorités compétentes leur participation aux accords de partage d'informations en matière de cybersécurité visés au paragraphe 2, lorsqu'elles concluent de tels accords ou, le cas échéant, lorsqu'elles se retirent de ces accords, une fois que le retrait prend effet.		
N/A	Art. 29, 5. L'ENISA fournit une assistance pour la mise en place des accords de partage d'informations en matière de cybersécurité visés au paragraphe 2 par l'échange de bonnes pratiques et l'apport d'orientations.		
N/A	Art. 30, 1. Les États membres veillent à ce que, outre l'obligation de notification prévue à l'article 23, des notifications puissent être transmises à titre volontaire aux CSIRT ou, s'il y a lieu, aux autorités compétentes par:		Cf. Fiche d'impact « Notification d'incidents et partage d'informations ».

	a) les entités essentielles et importantes en ce qui concerne les incidents, les cybermenaces et les incidents évités; b) les entités autres que celles visées au point a), indépendamment du fait qu'elles relèvent ou non du champ d'application de la présente directive, en ce qui concerne les incidents importants, les cybermenaces ou les incidents évités.		
N/A	Art. 30, 2. Les États membres traitent les notifications visées au paragraphe 1 du présent article conformément à la procédure énoncée à l'article 23. Les États membres peuvent traiter les notifications obligatoires en leur donnant la priorité par rapport aux notifications volontaires. Lorsque cela est nécessaire, les CSIRT et, le cas échéant, les autorités compétentes fournissent aux points de contact uniques les informations relatives aux notifications reçues en vertu du présent article, tout en garantissant la confidentialité et une protection appropriée des informations fournies par l'entité à l'origine de la notification. Sans préjudice de la prévention et de la détection d'infractions pénales et des enquêtes et poursuites en la matière, un signalement volontaire n'a pas pour effet d'imposer à l'entité ayant effectué la notification		Cf. Fiche d'impact « Notification d'incidents et partage d'informations ».

	des obligations supplémentaires auxquelles elle n'aurait pas été soumise si elle n'avait pas transmis la notification.		
N/A	Art. 31, 1. Les États membres veillent à ce que leurs autorités compétentes procèdent à une supervision efficace et prennent les mesures nécessaires pour assurer le respect de la présente directive.		
N/A	Art. 31, 2. Les États membres peuvent autoriser leurs autorités compétentes à fixer des priorités en ce qui concerne les tâches de supervision. La définition de ces priorités suit une approche basée sur les risques. À cet effet, lorsqu'elles accomplissent leurs tâches de supervision prévues aux articles 32 et 33, les autorités compétentes peuvent mettre au point des méthodes de supervision permettant de fixer des priorités concernant ces tâches selon une approche basée sur les risques.		
N/A	Art. 31, 3. Lorsqu'elles traitent des incidents donnant lieu à des violations de données à caractère personnel, les autorités compétentes coopèrent étroitement avec		

	les autorités de contrôle en vertu du règlement (UE) 2016/679, sans préjudice de la compétence et des missions des autorités de contrôle.		
N/A	Art. 31, 4. Sans préjudice des cadres législatifs et institutionnels nationaux, les États membres veillent à ce que, dans le cadre de la supervision du respect de la présente directive par les entités de l'administration publique et de l'imposition d'éventuelles mesures d'exécution en cas de violation de la présente directive, les autorités compétentes disposent de pouvoirs appropriés pour mener à bien ces tâches en jouissant d'une indépendance opérationnelle vis-à-vis des entités de l'administration publique supervisées. Les États membres peuvent décider d'imposer des mesures de supervision et d'exécution appropriées, proportionnées et efficaces à l'égard de ces entités, conformément aux cadres législatifs et institutionnels nationaux.		
N/A	Art. 32, 1. Les États membres veillent à ce que les mesures de supervision ou d'exécution imposées aux entités essentielles à l'égard des obligations prévues par la présente directive soient effectives, proportionnées et dissuasives, compte tenu des circonstances de		

	chaque cas.		
Art. 29 Le contrôle de l'autorité nationale de sécurité des systèmes d'information peut prendre la forme suivante : 1° Inspections sur place et contrôles à distance ; 2° Audits de sécurité réguliers et ciblés réalisés par l'autorité nationale mentionnée au premier alinéa ou par un organisme indépendant choisi par cette dernière ; 3° Scans de sécurité ; 4° Audits en cas d'incident important ou d'une violation des dispositions de l'article 26. Le coût de ces mesures est à la charge des personnes contrôlées sauf lorsque, à titre exceptionnel, l'autorité nationale de sécurité des systèmes d'information en décide autrement.	<u>Art. 32, 2.</u> 1) Les États membres veillent à ce que les autorités compétentes, lorsqu'elles accomplissent leurs tâches de supervision à l'égard d'entités essentielles, aient le pouvoir de soumettre ces entités à, au minimum : a) des inspections sur place et des contrôles à distance, y compris des contrôles aléatoires effectués par des professionnels formés; b) des audits de sécurité réguliers et ciblés réalisés par un organisme indépendant ou une autorité compétente; c) des audits ad hoc, notamment lorsqu'ils sont justifiés en raison d'un incident important ou d'une violation de la présente directive par l'entité essentielle; d) des scans de sécurité fondés sur des critères d'évaluation des risques objectifs, non discriminatoires, équitables et transparents, si nécessaire avec la coopération de l'entité concernée; e) des demandes d'informations nécessaires à l'évaluation des mesures de gestion des risques en matière de cybersécurité adoptées par l'entité concernée, notamment les politiques de		Cf. Fiche d'impact « Supervision – Procédures de contrôle et de sanction ».

	cybersécurité consignées par écrit, ainsi que du respect de l'obligation de soumettre des informations aux autorités compétentes conformément à l'article 27; f) des demandes d'accès à des données, à des documents et à toutes informations nécessaires à l'accomplissement de leurs tâches de supervision; g) des demandes de preuves de la mise en œuvre de politiques de cybersécurité, telles que les résultats des audits de sécurité effectués par un auditeur qualifié et les éléments de preuve sous-jacents correspondants. Les audits de sécurité ciblés visés au premier alinéa, point b), sont basés sur des évaluations des risques effectuées par l'autorité compétente ou l'entité contrôlée, ou sur d'autres informations disponibles relatives aux risques. Les résultats de tout audit de sécurité ciblé sont mis à la disposition de l'autorité compétente. Les coûts de cet audit de sécurité ciblé effectué par un organisme indépendant sont à la charge de l'entité contrôlée, sauf lorsque l'autorité compétente en décide autrement dans des cas dûment motivés.		
Art. 30 Les modalités d'application de la présente section sont	Art. 32, 3. Lorsqu'elles exercent leurs pouvoirs en vertu du	Norme de niveau	Cf. Fiche d'impact « Supervision –

précisées par décret en Conseil d'Etat.	paragraphe 2, point e), f) ou g), les autorités compétentes mentionnent la finalité de la demande et précisent quelles sont les informations exigées.	législatif, qui sera à décliner par un décret.	Procédures de contrôle et de sanction ».
Art. 32 Lorsque cette instruction ne fait pas état de faits justifiant une mesure d'exécution, l'autorité nationale de sécurité des systèmes d'information clôt la procédure et en informe la personne concernée. Dans le cas contraire, l'autorité nationale peut, après avoir mis la personne concernée en mesure de présenter ses observations : 1° Prononcer une mise en garde à son encontre ; 2° Lui enjoindre de prendre les mesures nécessaires pour éviter un incident ou y remédier, et définir les délais pour mettre en œuvre ces mesures et rendre compte de cette mise en œuvre ; 3° 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 grave ou répété ; 4° Lui ordonner d'informer les personnes physiques ou morales à l'égard desquelles elle fournit des	Art. 32, 4. 3) Les États membres veillent à ce que leurs autorités compétentes, lorsqu'elles exercent leurs pouvoirs d'exécution à l'égard d'entités essentielles, aient au minimum le pouvoir: a) d'émettre des avertissements concernant les violations de la présente directive par les entités concernées; b) 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 présente directive; c) d'ordonner aux entités concernées de mettre un terme à un comportement qui viole la présente directive et de ne pas le réitérer; d) d'ordonner aux entités concernées de garantir la conformité de leurs mesures de		Cf. Fiche d'impact « Supervision – Procédures de contrôle et de sanction ».

services ou exerce des activités susceptibles d'être affectées par une cybermenace importante, de la nature de cette menace, ainsi que de toutes mesures préventives ou réparatrices que ces personnes physiques ou morales pourraient prendre en réponse à cette menace ; 5° Lui enjoindre de mettre en œuvre dans le délai qu'elle fixe les recommandations formulées à la suite d'un audit de sécurité ; 6° Exiger qu'elle communique au public le manquement constaté par tout moyen adapté. La mesure d'exécution est notifiée aux intéressés et assortie, le cas échéant, d'une astreinte dont le montant ne peut excéder 5 000 euros par jour de retard. L'autorité nationale de la sécurité des systèmes d'information peut décider de la rendre publique. L'astreinte journalière court à compter du jour suivant l'expiration du délai imparti aux personnes concernées pour déférer à l'injonction. En cas d'inexécution totale ou partielle ou d'exécution tardive, la commission des sanctions mentionnée à l'article 35 peut procéder à la liquidation de l'astreinte.	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; e) 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; f) d'ordonner aux entités concernées de mettre en œuvre les recommandations formulées à la suite d'un audit de sécurité dans un délai raisonnable; g) de 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; h) d'ordonner aux entités concernées de rendre publics les aspects de violations de la présente directive de manière spécifique; i) d'imposer ou de demander aux organes compétents ou aux juridictions d'imposer, conformément au droit national, une amende administrative en vertu de l'article 34 en plus de		

	l'une ou l'autre des mesures visées aux points a) à h) du présent paragraphe.		
Art. 32, premier et second alinéa Lorsque cette instruction ne fait pas état de faits justifiant une mesure d'exécution, l'autorité nationale de sécurité des systèmes d'information clôt la procédure et en informe la personne concernée. Dans le cas contraire, l'autorité nationale peut, après avoir mis la personne concernée en mesure de présenter ses observations : 1° Prononcer une mise en garde à son encontre ; 2° Lui enjoindre de prendre les mesures nécessaires pour éviter un incident ou y remédier, et définir les délais pour mettre en œuvre ces mesures et rendre compte de cette mise en œuvre ; 3° 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 grave ou répété ; 4° Lui ordonner d'informer les personnes physiques ou morales à l'égard desquelles elle fournit des services ou exerce des activités susceptibles d'être affectées par une cybermenace importante, de la nature de cette menace, ainsi que de toutes mesures préventives ou réparatrices que ces personnes physiques ou morales pourraient prendre en réponse à cette menace ; 5° Lui enjoindre de mettre en œuvre	Art. 32, 5. Lorsque les mesures d'exécution adoptées en vertu du paragraphe 4, points a) à d) et point f), 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 : a) de suspendre temporairement ou de demander à un organisme de certification ou d'autorisation, ou à une juridiction, conformément au droit national, de suspendre temporairement une certification ou une autorisation concernant tout ou partie des services pertinents fournis ou des activités pertinentes menées par l'entité essentielle; b) de demander aux organes compétents ou aux juridictions compétentes, conformément au droit national, d'interdire temporairement à toute personne physique exerçant des responsabilités dirigeantes à un niveau de directeur général ou		Cf. Fiche d'impact « Supervision – Procédures de contrôle et de sanction ».

dans le délai qu'elle fixe les recommandations formulées à la suite d'un audit de sécurité ; 6° Exiger qu'elle communique au public le manquement constaté par tout moyen adapté. Art. 33 Lorsque la personne concernée apporte les éléments montrant qu'elle s'est conformée à la mesure d'exécution mentionnée à l'article 32 dans le délai imparti, l'autorité nationale de sécurité des systèmes d'information constate qu'il n'y a pas lieu de poursuivre la procédure et le notifie à cette personne. Lorsque la personne en cause ne se conforme pas à l'une des mesures d'exécution qui lui est adressée, l'autorité nationale de sécurité des systèmes d'information lui notifie les griefs et saisit la commission des sanctions mentionnée à l'article 35. Lorsque la personne concernée est une entité essentielle et qu'elle n'apporte pas la preuve qu'elle s'est conformée aux mesures d'exécution mentionnées aux 1° à 3° et 5° de l'article 32 dans le délai imparti, l'autorité nationale de sécurité des systèmes d'information peut suspendre une certification ou une autorisation concernant tout ou partie des services fournis ou des activités exercées par l'entité jusqu'à ce que l'entité essentielle ait remédié au manquement. Lorsque cette certification ou cette autorisation a été	de représentant légal dans l'entité essentielle d'exercer des responsabilités dirigeantes dans cette entité. Les suspensions ou interdictions temporaires imposées au titre du présent paragraphe sont uniquement appliquées jusqu'à ce que l'entité concernée prenne les mesures nécessaires pour remédier aux insuffisances ou se conformer aux exigences de l'autorité compétente à l'origine de l'application de ces mesures d'exécution. L'imposition de ces suspensions ou interdictions temporaires est soumise à des garanties procédurales appropriées conformément aux principes généraux du droit de l'Union et à la Charte, y compris le droit à un recours effectif et à accéder à un tribunal impartial, la présomption d'innocence et les droits de la défense. Les mesures d'exécution prévues au présent paragraphe ne peuvent pas être appliquées aux entités de l'administration publiques qui relèvent de la présente directive.		

délivrée par à un organisme de certification ou d'autorisation par un autre organisme, elle enjoint à cet organisme de la suspendre jusqu'à ce que l'entité essentielle ait remédié au manquement. Art. 37, V. V. – 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. Ces dispositions ne s'appliquent pas aux administrations.			
Art. 37, V. V. – 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. Ces dispositions ne s'appliquent pas aux administrations.	Art. 32, 6. Les États membres veillent à ce que toute personne physique responsable d'une entité essentielle ou agissant en qualité de représentant légal d'une entité essentielle sur la base du pouvoir de la représenter, de prendre des décisions en son nom ou d'exercer son contrôle ait le pouvoir de veiller au respect, par l'entité, de la présente directive. Les États membres veillent à ce que ces personnes physiques puissent être tenues responsables des manquements à leur devoir de veiller au respect de la présente directive. En ce qui concerne les entités de l'administration publique, le présent paragraphe est sans préjudice		Cf. Fiche d'impact « Supervision – Procédures de contrôle et de sanction ».

	du droit national en ce qui concerne la responsabilité des agents de la fonction publique et des responsables élus ou nommés.		
Art. 34 Un décret en Conseil d'Etat fixe les modalités de la procédure prévue à la présente section.	<u>Art. 32, 7.</u> 1) Lorsqu'elles prennent toute mesure d'exécution visée au paragraphe 4 ou 5, les autorités compétentes respectent les droits de la défense et tiennent compte des circonstances propres à chaque cas et, au minimum, tiennent dûment compte: a) de la gravité de la violation et de l'importance des dispositions enfreintes, les faits suivants, entre autres, devant être considérés en tout état de cause comme graves: i. les violations répétées; ii. le fait de ne pas notifier des incidents importants ou de ne pas y remédier; iii. le fait de ne pas pallier les insuffisances à la suite d'instructions contraignantes des autorités compétentes; iv. le fait d'entraver des audits ou des activités de contrôle ordonnées par l'autorité compétente à la suite de la constatation d'une violation; v. la fourniture d'informations fausses ou manifestement inexactes relatives aux	Norme de niveau législatif, qui sera à décliner par un décret.	Cf. Fiche d'impact « Supervision – Procédures de contrôle et de sanction ».

	mesures de gestion des risques en matière de cybersécurité ou aux obligations d'information prévues aux articles 21 et 23; b) de la durée de la violation; b) de toute violation antérieure pertinente commise par l'entité concernée; c) des dommages matériels, corporels ou moraux causés, y compris des pertes financières ou économiques, des effets sur d'autres services et du nombre d'utilisateurs touchés; d) du fait que l'auteur de la violation a agi délibérément ou par négligence; e) des mesures prises par l'entité pour prévenir ou atténuer les dommages matériels, corporels ou moraux; f) de l'application de codes de conduite approuvés ou de mécanismes de certification approuvés; g) du degré de coopération avec les autorités compétentes des personnes physiques ou morales tenues pour responsables.		
Art. 32, premier et second alinéa Lorsque cette instruction ne fait pas état de faits justifiant une mesure d'exécution, l'autorité nationale de sécurité des systèmes d'information clôt la	Art. 32, 8. Les autorités compétentes exposent en détail les motifs de leurs mesures d'exécution. Avant de prendre de telles mesures, les autorités compétentes		Cf. Fiche d'impact « Supervision – Procédures de contrôle et de sanction ».

procédure et en informe la personne concernée. Dans le cas contraire, l'autorité nationale peut, après avoir mis la personne concernée en mesure de présenter ses observations : 1° Prononcer une mise en garde à son encontre ; 2° Lui enjoindre de prendre les mesures nécessaires pour éviter un incident ou y remédier, et définir les délais pour mettre en œuvre ces mesures et rendre compte de cette mise en œuvre ; 3° 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 grave ou répété ; 4° Lui ordonner d'informer les personnes physiques ou morales à l'égard desquelles elle fournit des services ou exerce des activités susceptibles d'être affectées par une cybermenace importante, de la nature de cette menace, ainsi que de toutes mesures préventives ou réparatrices que ces personnes physiques ou morales pourraient prendre en réponse à cette menace ; 5° Lui enjoindre de mettre en œuvre dans le délai qu'elle fixe les recommandations formulées à la suite d'un audit de sécurité ; 6° Exiger qu'elle communique au public le manquement constaté par tout moyen adapté.	informent les entités concernées de leurs conclusions préliminaires. Elles laissent en outre à ces entités un délai raisonnable pour communiquer leurs observations, sauf dans des cas exceptionnels dûment motivés où cela empêcherait une intervention immédiate pour prévenir un incident ou y répondre.		
N/A	Art. 32, 9.		N/A

	Les États membres veillent à ce que leurs autorités compétentes en vertu de la présente directive informent les autorités compétentes concernées au sein du même État membre en vertu de la directive (UE) 2022/2557 lorsqu'elles exercent leurs pouvoirs de supervision et d'exécution dans le but de garantir qu'une entité définie comme critique en vertu de la directive (UE) 2022/2557 respecte la présente directive. S'il y a lieu, les autorités compétentes en vertu de la directive (UE) 2022/2557 peuvent demander aux autorités compétentes en vertu de la présente directive d'exercer leurs pouvoirs de supervision et d'exécution à l'égard d'une entité qui est définie comme entité critique en vertu de la directive (UE) 2022/ 2557.		
Art. 23 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'autorité nationale de sécurité des systèmes d'information, et, d'autre part, la Commission nationale de l'informatique et des	<u>Art. 32, 10.</u> Les États membres veillent à ce que leurs autorités compétentes en vertu de la présente directive coopèrent avec les autorités compétentes pertinentes de l'État membre concerné au titre du règlement (UE) 2022/2554. Les États membres veillent, en particulier, à ce que leurs autorités compétentes en vertu de la présente directive informent le forum de supervision institué en vertu de l'article 32, paragraphe 1, du règlement (UE) 2022/2554 lorsqu'elles exercent leurs pouvoirs de supervision et d'exécution dans le but de garantir	Norme de niveau législatif, qui sera à décliner par un décret.	Cf. Fiche d'impact « Notifications d'incidents importants et partage d'informations ».

libertés 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 Etats membres de l'Union européenne ou des centres de réponse aux incidents de sécurité informatique ou des organismes internationaux concourant aux missions de sécurité ou de défense des systèmes d'information. Les modalités d'application du présent article, notamment les modalités du partage d'informations, sont déterminées par décret en Conseil d'Etat.	qu'une entité essentielle qui a été désignée comme étant un prestataire tiers critique de services TIC au titre de l'article 31 du règlement (UE) 2022/2554 respecte la présente directive.		
Art. 29 Le contrôle de l'autorité nationale de sécurité des systèmes d'information peut prendre la forme suivante : 1° Inspections sur place et contrôles à distance ; 2° Audits de sécurité réguliers et ciblés réalisés par l'autorité nationale mentionnée au premier alinéa ou par un organisme indépendant choisi par cette dernière ; 3° Scans de sécurité ;	Art. 33, 1. Au vu d'éléments de preuve, d'indications ou d'informations selon lesquels une entité importante ne respecterait pas la présente directive, et notamment ses articles 21 et 23, les États membres veillent à ce que les autorités compétentes prennent des mesures, le cas échéant, dans le cadre de mesures de contrôle ex post. Les États membres veillent à ce que ces mesures soient effectives, proportionnées et dissuasives, compte tenu des circonstances propres à chaque cas d'espèce.		Cf. Fiche d'impact « Supervision – Procédures de contrôle et de sanction ».

4° Audits en cas d'incident important ou d'une violation des dispositions de l'article 26. Le coût de ces mesures est à la charge des personnes contrôlées sauf lorsque, à titre exceptionnel, l'autorité nationale de sécurité des systèmes d'information en décide autrement. Art. 32 Lorsque cette instruction ne fait pas état de faits justifiant une mesure d'exécution, l'autorité nationale de sécurité des systèmes d'information clôt la procédure et en informe la personne concernée. Dans le cas contraire, l'autorité nationale peut, après avoir mis la personne concernée en mesure de présenter ses observations : 1° Prononcer une mise en garde à son encontre ; 2° Lui enjoindre de prendre les mesures nécessaires pour éviter un incident ou y remédier, et définir les délais pour mettre en œuvre ces mesures et rendre compte de cette mise en œuvre ; 3° 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 grave ou répété ;			

4° Lui ordonner d'informer les personnes physiques ou morales à l'égard desquelles elle fournit des services ou exerce des activités susceptibles d'être affectées par une cybermenace importante, de la nature de cette menace, ainsi que de toutes mesures préventives ou réparatrices que ces personnes physiques ou morales pourraient prendre en réponse à cette menace ; 5° Lui enjoindre de mettre en œuvre dans le délai qu'elle fixe les recommandations formulées à la suite d'un audit de sécurité ; 6° Exiger qu'elle communique au public le manquement constaté par tout moyen adapté. La mesure d'exécution est notifiée aux intéressés et assortie, le cas échéant, d'une astreinte dont le montant ne peut excéder 5 000 euros par jour de retard. L'autorité nationale de la sécurité des systèmes d'information peut décider de la rendre publique. L'astreinte journalière court à compter du jour suivant l'expiration du délai imparti aux personnes concernées pour déférer à l'injonction. En cas d'inexécution totale ou partielle ou d'exécution tardive, la commission des sanctions mentionnée à l'article 35 peut procéder à la liquidation de l'astreinte.			

Art. 29 Le contrôle de l'autorité nationale de sécurité des systèmes d'information peut prendre la forme suivante : 1° Inspections sur place et contrôles à distance ; 2° Audits de sécurité réguliers et ciblés réalisés par l'autorité nationale mentionnée au premier alinéa ou par un organisme indépendant choisi par cette dernière ; 3° Scans de sécurité ; 4° Audits en cas d'incident important ou d'une violation des dispositions de l'article 26. Le coût de ces mesures est à la charge des personnes contrôlées sauf lorsque, à titre exceptionnel, l'autorité nationale de sécurité des systèmes d'information en décide autrement.	<u>Art. 33, 2.</u> Les États membres veillent à ce que les autorités compétentes, lorsqu'elles accomplissent leurs tâches de supervision à l'égard d'entités importantes, aient le pouvoir de soumettre ces entités, au minimum, à : a) des inspections sur place et des contrôles à distance ex post, effectués par des professionnels formés; b) des audits de sécurité ciblés réalisés par un organisme indépendant ou une autorité compétente ; c) des scans de sécurité fondés sur des critères d'évaluation des risques objectifs, non discriminatoires, équitables et transparents, si nécessaire avec la coopération de l'entité concernée ; d) des demandes d'informations nécessaires à l'évaluation ex post des mesures de gestion des risques en matière de cybersécurité adoptées par l'entité concernée, notamment les politiques de cybersécurité consignées par écrit, ainsi que du respect de l'obligation de soumettre des informations aux autorités compétentes conformément à l'article 27 ; e) des demandes d'accès à des données, à des		Cf. Fiche d'impact « Supervision – Procédures de contrôle et de sanction ».

	documents et à des informations nécessaires à l'accomplissement de leurs tâches de supervision ; f) des demandes de preuves de la mise en œuvre de politiques de cybersécurité, telles que les résultats des audits de sécurité effectués par un auditeur qualifié et les éléments de preuve sous-jacents correspondants. Les audits de sécurité ciblés visés au premier alinéa, point b), sont fondés sur des évaluations des risques effectuées par l'autorité compétente ou l'entité contrôlée, ou sur d'autres informations disponibles relatives aux risques. Les résultats de tout audit de sécurité ciblé sont mis à la disposition de l'autorité compétente. Les coûts de cet audit de sécurité ciblé effectué par un organisme indépendant sont à la charge de l'entité contrôlée, sauf lorsque l'autorité compétente en décide autrement dans des cas dûment motivés.		
Art. 31 Au vu des résultats du contrôle réalisé en application des dispositions de la section 1, l'autorité nationale de sécurité des systèmes d'information peut décider de l'ouverture d'une procédure à l'encontre de la personne contrôlée. Elle lui notifie sa décision. L'autorité nationale de sécurité des systèmes	Art. 33, 3. Lorsqu'elles exercent leurs pouvoirs en vertu du paragraphe 2, point d), e) ou f), les autorités compétentes mentionnent la finalité de la demande et précisent quelles sont les informations exigées.		Cf. Fiche d'impact « Supervision – Procédures de contrôle et de sanction ».

d'information désigne parmi les agents et personnes mentionnés à l'article 26 un ou plusieurs rapporteurs chargés de l'instruction de cette procédure.			
Art. 32 Lorsque cette instruction ne fait pas état de faits justifiant une mesure d'exécution, l'autorité nationale de sécurité des systèmes d'information clôt la procédure et en informe la personne concernée. Dans le cas contraire, l'autorité nationale peut, après avoir mis la personne concernée en mesure de présenter ses observations : 1° Prononcer une mise en garde à son encontre ; 2° Lui enjoindre de prendre les mesures nécessaires pour éviter un incident ou y remédier, et définir les délais pour mettre en œuvre ces mesures et rendre compte de cette mise en œuvre ; 3° 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 grave ou répété ; 4° Lui ordonner d'informer les personnes physiques ou morales à l'égard desquelles elle fournit des services ou exerce des activités susceptibles d'être affectées par une cybermenace importante, de la	<u>Art. 33, 4.</u> 4) Les États membres veillent à ce que les autorités compétentes, lorsqu'elles exercent leurs pouvoirs d'exécution à l'égard d'entités importantes, aient au minimum le pouvoir: a) d'émettre des avertissements concernant des violations de la présente directive par les entités concernées ; b) d'adopter des instructions contraignantes ou une injonction exigeant des entités concernées qu'elles pallient les insuffisances constatées ou les violations de la présente directive ; c) d'ordonner aux entités concernées de mettre un terme à un comportement qui viole la présente directive et de ne pas le réitérer ; d) 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 prévues à l'article 23, de manière spécifique et dans un délai déterminé; e) d'ordonner aux entités concernées d'informer les personnes physiques ou morales à		Cf. Fiche d'impact « Supervision – Procédures de contrôle et de sanction ».

nature de cette menace, ainsi que de toutes mesures préventives ou réparatrices que ces personnes physiques ou morales pourraient prendre en réponse à cette menace ; 5° Lui enjoindre de mettre en œuvre dans le délai qu'elle fixe les recommandations formulées à la suite d'un audit de sécurité ; 6° Exiger qu'elle communique au public le manquement constaté par tout moyen adapté. La mesure d'exécution est notifiée aux intéressés et assortie, le cas échéant, d'une astreinte dont le montant ne peut excéder 5 000 euros par jour de retard. L'autorité nationale de la sécurité des systèmes d'information peut décider de la rendre publique. L'astreinte journalière court à compter du jour suivant l'expiration du délai imparti aux personnes concernées pour déférer à l'injonction. En cas d'inexécution totale ou partielle ou d'exécution tardive, la commission des sanctions mentionnée à l'article 35 peut procéder à la liquidation de l'astreinte.	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; f) d'ordonner aux entités concernées de mettre en œuvre les recommandations formulées à la suite d'un audit de sécurité dans un délai raisonnable; g) d'ordonner aux entités concernées de rendre publics des aspects de violations de la présente directive de manière spécifique; h) d'imposer ou de demander aux organes compétents ou aux juridictions compétentes d'imposer, conformément au droit national, une amende administrative en vertu de l'article 34 en plus de l'une ou l'autre des mesures visées aux points a) à g) du présent paragraphe.		
Art. 34 Un décret en Conseil d'Etat fixe les modalités de la procédure prévue à la présente section.	<u>Art. 33, 5.</u> L'article 32, paragraphes 6, 7 et 8, s'applique mutatis mutandis aux mesures de supervision et d'exécution prévues au présent article pour les	Norme de niveau législatif, qui sera à décliner par	Cf. Fiches d'impact – « Périmètre de compétence de l'autorité nationale et

	entités importantes.	un décret.	exigences de sécurité » – « Supervision – Procédures de contrôle et de sanction ».
Art. 23 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'autorité nationale de sécurité des systèmes d'information, et, d'autre part, la Commission nationale de l'informatique et des libertés 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 Etats membres de l'Union européenne ou des centres de réponse aux incidents de sécurité	Art. 33, 6. Les États membres veillent à ce que leurs autorités compétentes en vertu de la présente directive coopèrent avec les autorités compétentes pertinentes de l'État membre concerné au titre du règlement (UE) 2022/2554. Les États membres veillent, en particulier, à ce que leurs autorités compétentes au titre de la présente directive informent le forum de supervision établi en vertu de l'article 32, paragraphe 1, du règlement (UE) 2022/2554 lorsqu'elles exercent leurs pouvoirs de supervision et d'exécution dans le but de garantir qu'une entité importante qui a été désignée comme étant un prestataire tiers critique de services TIC en vertu de l'article 31 du règlement (UE) 2022/2554 respecte la présente directive.	Norme de niveau législatif, qui sera à décliner par un décret.	Cf. Fiche d'impact « Notification d'incidents et partage d'informations ».

informatique ou des organismes internationaux concourant aux missions de sécurité ou de défense des systèmes d'information. Les modalités d'application du présent article, notamment les modalités du partage d'informations, sont déterminées par décret en Conseil d'Etat.			
Art. 35 La commission des sanctions mentionnée à l'article L. 1332-15 du code de la défense statue sur les manquements constatés aux obligations découlant de l'application des chapitres II et III du présent titre, dans les conditions prévues par la présente section. Art. 36 Lorsqu'elle est saisie de manquements aux obligations découlant de l'application des chapitres II et III du présent titre, la commission des sanctions est composée : 1° Des personnes mentionnées au 1° de l'article L. 1332-16 du code de la défense ; 2° De trois personnalités qualifiées, nommées par le Premier ministre en raison de leurs compétences dans le domaine de la sécurité des systèmes d'information. Art. 37 I. – En cas de manquement constaté aux obligations prévues par les dispositions prévues au présent titre, la	Art. 34, 1. Les États membres veillent à ce que les amendes administratives imposées aux entités essentielles et importantes en vertu du présent article pour des violations de la présente directive soient effectives, proportionnées et dissuasives, compte tenu des circonstances de chaque cas.		Cf. Fiche d'impact « Supervision – Procédures de contrôle et de sanction ».

commission des sanctions peut prononcer : 1° A l'encontre des entités essentielles et des opérateurs mentionnés à l'article L. 1332-2 du code de la défense, à l'exception des administrations de l'Etat et de ses établissements publics administratifs, des collectivités territoriales, de leurs groupements et de leurs établissements publics administratifs, une amende administrative dont le montant, proportionné à la gravité du manquement, ne peut excéder 10 millions d'euros ou 2 % du chiffre d'affaires annuel mondial, hors taxes, de l'exercice précédent de l'entreprise à laquelle l'entité essentielle appartient, le montant le plus élevé étant retenu ; 2° A l'encontre des entités importantes, à l'exception des administrations de l'Etat et de ses établissements publics administratifs, des collectivités territoriales, de leurs groupements et de leurs établissements publics administratifs, une amende administrative dont le montant, proportionné à la gravité du manquement, ne peut excéder 7 millions d'euros ou 1,4 % du chiffre d'affaires annuel mondial total, hors taxes, de l'exercice précédent de l'entreprise à laquelle l'entité importante appartient, le montant le plus élevé étant retenu ; 3° A l'encontre des offices d'enregistrement et des bureaux d'enregistrement mentionnés à l'article 18 de la présente loi, à l'exception de ceux relevant des articles L. 45 à L. 45-8 du code des postes et des communications électroniques lorsqu'il s'agit d'un			

manquement aux obligations prévues à la section 3 du chapitre II de la présente loi, une amende administrative dont le montant, proportionné à la gravité du manquement, ne peut excéder 7 millions d'euros ou 1,4 % du chiffre d'affaires annuel mondial total, hors taxes, de l'exercice précédent. Cette amende peut se cumuler avec l'amende prévue au 1° prononcée à l'encontre d'un office d'enregistrement en cas de manquement aux obligations applicables aux entités essentielles. Si les manquements relevés constituent également une violation du règlement (UE) n° 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE, donnant lieu à un amende administrative prononcée par la Commission nationale de l'informatique et des libertés en vertu des articles 20 à 22-1 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, la commission des sanctions ne peut prononcer de sanction sous forme d'amende administrative. II. – La commission des sanctions peut prononcer une amende administrative dont le montant, proportionné à la gravité du manquement, ne peut excéder 10 millions d'euros ou 2 % du chiffre d'affaires annuel mondial total, hors taxes, de l'exercice précédent, le montant le plus élevé étant retenu, à l'encontre : 1° Des fournisseurs de moyens d'identification			

électronique relevant des schémas d'identification électronique notifiés par l'Etat, des prestataires de services de confiance établis sur le territoire français, des fournisseurs de dispositifs de création de signature et de cachet électronique qualifié qu'elle certifie et des organismes d'évaluation de la conformité, à l'exception des administrations de l'Etat et de leurs établissements publics à caractère administratif, en cas de manquement constaté aux dispositions du règlement (UE) n° 910/2014 du 23 juillet 2014 mentionné ci-dessus ; 2° Des organismes d'évaluation de la conformité sauf si l'organisme d'évaluation de la conformité est l'autorité nationale de certification de cybersécurité, des titulaires d'une déclaration de conformité aux exigences d'un schéma de certification européen, des titulaires d'un agrément, d'une qualification ou d'un certificat dans le domaine de la cybersécurité, en cas de manquement constaté aux dispositions du règlement (UE) n° 2019/881 du 17 avril 2019 mentionné ci-dessus ou aux exigences applicables mentionnés au 4° et au 5° de l'article 26 de la présente loi. III. – Lorsque la commission des sanctions envisage également de prononcer l'amende prévue à l'article 28 à l'encontre de la même personne, le montant cumulé des sanctions ne peut excéder le montant maximum de l'amende prévue au I ou au II du présent article. IV. – La commission des sanctions peut également			

prononcer les mesures suivantes à l'encontre des organismes d'évaluation de la conformité et des titulaires d'agréments, de qualifications ou de certificats en matière de cybersécurité, au titre des dispositions du règlement (UE) n° 910/2014 du 23 juillet 2014 mentionné ci-dessus, des dispositions du règlement (UE) 2019/881 du 17 avril 2019 mentionné ci-dessus ou des exigences de cybersécurité mentionnés au 5° de l'article 26 de la présente loi : 1° L'abrogation d'un agrément, d'une qualification ou d'un certificat ; 2° L'abrogation de l'autorisation, de l'agrément ou de l'habilitation délivré à l'organisme d'évaluation de la conformité, lorsque le manquement n'est pas corrigé dans le délai imparti par l'autorité nationale de sécurité des systèmes d'information. V. – 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. Ces dispositions ne s'appliquent pas aux administrations.			
Art. 33 Lorsque la personne concernée apporte les éléments montrant qu'elle s'est conformée à la mesure d'exécution mentionnée à l'article 32 dans le délai	Art. 34, 2. Les amendes administratives sont imposées en complément de l'une ou l'autre des mesures visées à l'article 32, paragraphe 4, points a) à h), à		Cf. Fiche d'impact « Supervision – Procédures de contrôle et de sanction ».

imparti, l'autorité nationale de sécurité des systèmes d'information constate qu'il n'y a pas lieu de poursuivre la procédure et le notifie à cette personne. Lorsque la personne en cause ne se conforme pas à l'une des mesures d'exécution qui lui est adressée, l'autorité nationale de sécurité des systèmes d'information lui notifie les griefs et saisit la commission des sanctions mentionnée à l'article 35. Lorsque la personne concernée est une entité essentielle et qu'elle n'apporte pas la preuve qu'elle s'est conformée aux mesures d'exécution mentionnées aux 1° à 3° et 5° de l'article 32 dans le délai imparti, l'autorité nationale de sécurité des systèmes d'information peut suspendre une certification ou une autorisation concernant tout ou partie des services fournis ou des activités exercées par l'entité jusqu'à ce que l'entité essentielle ait remédié au manquement. Lorsque cette certification ou cette autorisation a été délivrée par à un organisme de certification ou d'autorisation par un autre organisme, elle enjoint à cet organisme de la suspendre jusqu'à ce que l'entité essentielle ait remédié au manquement.	l'article 32, paragraphe 5, et à l'article 33, paragraphe 4, points a) à g).		
Art. 34 Un décret en Conseil d'Etat fixe les modalités de la procédure prévue à la présente section. Art. 35	Art. 34, 3. Au moment de décider s'il y a lieu d'imposer une amende administrative et de décider de son montant, dans chaque cas d'espèce, il est dûment tenu compte, au minimum, des éléments prévus à	Norme de niveau législatif, qui sera à décliner par	Cf. Fiche d'impact « Supervision – Procédures de contrôle et de sanction ».

La commission des sanctions mentionnée à l'article L. 1332-15 du code de la défense statue sur les manquements constatés aux obligations découlant de l'application des chapitres II et III du présent titre, dans les conditions prévues par la présente section. Art. 36 Lorsqu'elle est saisie de manquements aux obligations découlant de l'application des chapitres II et III du présent titre, la commission des sanctions est composée : 1° Des personnes mentionnées au 1° de l'article L. 1332-16 du code de la défense ; 2° De trois personnalités qualifiées, nommées par le Premier ministre en raison de leurs compétences dans le domaine de la sécurité des systèmes d'information.	l'article 32, paragraphe 7.	un décret.	
Art. 37, I., 1° I. – En cas de manquement constaté aux obligations prévues par les dispositions prévues au présent titre, la commission des sanctions peut prononcer : 1° A l'encontre des entités essentielles et des opérateurs mentionnés à l'article L. 1332-2 du code de la défense, à l'exception des administrations de l'Etat et de ses établissements publics administratifs, des collectivités territoriales, de leurs groupements et de	Art. 34, 4. Les États membres veillent à ce que, lorsqu'elles violent l'article 21 ou 23, les entités essentielles soient soumises, conformément aux paragraphes 2 et 3 du présent article, à des amendes administratives d'un montant maximal s'élevant à au moins 10 000 000 EUR ou à au moins 2 % du chiffre d'affaires annuel mondial total de l'exercice précédent de l'entreprise à laquelle l'entité		Cf. Fiche d'impact « Supervision – Procédures de contrôle et de sanction ».

leurs établissements publics administratifs, une amende administrative dont le montant, proportionné à la gravité du manquement, ne peut excéder 10 millions d'euros ou 2 % du chiffre d'affaires annuel mondial, hors taxes, de l'exercice précédent de l'entreprise à laquelle l'entité essentielle appartient, le montant le plus élevé étant retenu ;	essentielle appartient, le montant le plus élevé étant retenu.		
Art. 37, I., 2° 2° A l'encontre des entités importantes, à l'exception des administrations de l'Etat et de ses établissements publics administratifs, des collectivités territoriales, de leurs groupements et de leurs établissements publics administratifs, une amende administrative dont le montant, proportionné à la gravité du manquement, ne peut excéder 7 millions d'euros ou 1,4 % du chiffre d'affaires annuel mondial total, hors taxes, de l'exercice précédent de l'entreprise à laquelle l'entité importante appartient, le montant le plus élevé étant retenu ;	Art. 34, 5. Les États membres veillent à ce que, lorsqu'elles violent l'article 21 ou 23, les entités importantes soient soumises, conformément aux paragraphes 2 et 3 du présent article, à des amendes administratives d'un montant maximal s'élevant à au moins 7 000 000 EUR 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.		Cf. Fiche d'impact « Supervision – Procédures de contrôle et de sanction ».
Art. 32, quatrième et dernier alinéa La mesure d'exécution est notifiée aux intéressés et assortie, le cas échéant, d'une astreinte dont le montant ne peut excéder 5 000 euros par jour de retard. L'autorité nationale de la sécurité des systèmes d'information peut décider de la rendre publique. L'astreinte journalière court à compter du jour suivant l'expiration du délai imparti aux personnes concernées	Art. 34, 6. Les États membres peuvent prévoir le pouvoir d'imposer des astreintes pour contraindre une entité essentielle ou importante à mettre un terme à une violation de la présente directive conformément à une décision préalable de l'autorité compétente.		Cf. Fiche d'impact « Supervision – Procédures de contrôle et de sanction ».

pour déférer à l'injonction. En cas d'inexécution totale ou partielle ou d'exécution tardive, la commission des sanctions mentionnée à l'article 35 peut procéder à la liquidation de l'astreinte.			
Art. 37 I. – En cas de manquement constaté aux obligations prévues par les dispositions prévues au présent titre, la commission des sanctions peut prononcer : 1° A l'encontre des entités essentielles et des opérateurs mentionnés à l'article L. 1332-2 du code de la défense, à l'exception des administrations de l'Etat et de ses établissements publics administratifs, des collectivités territoriales, de leurs groupements et de leurs établissements publics administratifs, une amende administrative dont le montant, proportionné à la gravité du manquement, ne peut excéder 10 millions d'euros ou 2 % du chiffre d'affaires annuel mondial, hors taxes, de l'exercice précédent de l'entreprise à laquelle l'entité essentielle appartient, le montant le plus élevé étant retenu ; 2° A l'encontre des entités importantes, à l'exception des administrations de l'Etat et de ses établissements publics administratifs, des collectivités territoriales, de leurs groupements et de leurs établissements publics administratifs, une amende administrative dont le montant, proportionné à la gravité du manquement, ne	Art. 34, 7. Sans préjudice des pouvoirs des autorités compétentes en vertu des articles 32 et 33, 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.		Cf. Fiche d'impact « Supervision – Procédures de contrôle et de sanction ».

peut excéder 7 millions d'euros ou 1,4 % du chiffre d'affaires annuel mondial total, hors taxes, de l'exercice précédent de l'entreprise à laquelle l'entité importante appartient, le montant le plus élevé étant retenu ;			
N/A	Art. 34, 8. Si le système juridique d'un État membre ne prévoit pas d'amendes administratives, cet État membre veille à ce que le présent article soit appliqué de telle sorte que l'amende soit déterminée par l'autorité compétente et imposée par les juridictions nationales compétentes, tout en veillant à ce que ces voies de droit soit effectives et aient un effet équivalent aux amendes administratives imposées par les autorités compétentes. En tout état de cause, les amendes imposées sont effectives, proportionnées et dissuasives. L'État membre notifie à la Commission les dispositions légales qu'il adopte en vertu du présent paragraphe au plus tard le 17 octobre 2024 et, sans tarder, toute disposition légale modificative ou modification ultérieure les concernant.		
Art. 23 Les dispositions de l'article 11 du code de procédure pénale ou celles relatives aux autres secrets protégés	Art. 35, 1. Lorsque les autorités compétentes prennent connaissance, dans le cadre de la supervision ou de	Norme de niveau législatif, qui sera à	Cf. Fiche d'impact « Notification d'incidents et partage

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'autorité nationale de sécurité des systèmes d'information, et, d'autre part, la Commission nationale de l'informatique et des libertés 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 Etats membres de l'Union européenne ou des centres de réponse aux incidents de sécurité informatique ou des organismes internationaux concourant aux missions de sécurité ou de défense des systèmes d'information. Les modalités d'application du présent article, notamment les modalités du partage d'informations, sont déterminées par décret en Conseil d'Etat.	l'exécution, du fait que la violation commise par une entité essentielle ou importante à l'égard des obligations énoncées aux articles 21 et 23 de la présente directive peut donner lieu à une violation de données à caractère personnel au sens de l'article 4, point 12, du règlement (UE) 2016/679, devant être notifiée en vertu de l'article 33 dudit règlement, elles en informent sans retard injustifié les autorités de contrôle visées à l'article 55 ou 56 dudit règlement.	décliner par un décret.	d'informations ».
Art. 37, I. dernier alinéa I. – Si les manquements relevés constituent également une violation du règlement (UE) n° 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à	Art. 35, 2. Lorsque les autorités de contrôle visées à l'article 55 ou 56 du règlement (UE) 2016/679 imposent une amende administrative en vertu de l'article 58, paragraphe 2, point i), dudit règlement, les		Cf. Fiche d'impact « Supervision – Procédures de contrôle et de sanction ».

caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE, donnant lieu à un amende administrative prononcée par la Commission nationale de l'informatique et des libertés en vertu des articles 20 à 22-1 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, la commission des sanctions ne peut prononcer de sanction sous forme d'amende administrative.	autorités compétentes n'imposent pas d'amende administrative au titre de l'article 34 de la présente directive pour une violation visée au paragraphe 1 du présent article et découlant du même comportement que celui qui a fait l'objet d'une amende administrative au titre de l'article 58, paragraphe 2, point i), du règlement (UE) 2016/679. Les autorités compétentes peuvent toutefois imposer les mesures d'exécution prévues à l'article 32, paragraphe 4, points a) à h), à l'article 32, paragraphe 5, et à l'article 33, paragraphe 4, points a) à g), de la présente directive.		
N/A	Art. 35, 3. Lorsque l'autorité de contrôle compétente en vertu du règlement (UE) 2016/679 est établie dans un autre État membre que l'autorité compétente, l'autorité compétente informe l'autorité de contrôle établie dans son propre État membre de la violation potentielle de données à caractère personnel visée au paragraphe 1.		
N/A	Art. 36. 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. Les sanctions prévues sont effectives, proportionnées et dissuasives. Les États membres informent la Commission, au plus tard le 17 janvier 2025, des règles et mesures adoptées à cet égard, ainsi que, sans retard, de toute modification qui y serait apportée ultérieurement.		
Art. 23 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'autorité nationale de sécurité des systèmes d'information, et, d'autre part, la Commission nationale de l'informatique et des libertés 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 Etats membres de l'Union européenne ou des centres de réponse aux incidents de sécurité informatique ou des organismes internationaux	<u>Art. 37, 1.</u> Lorsqu'une entité fournit des services dans plusieurs États membres, ou fournit des services dans un ou plusieurs États membres alors que ses réseaux et systèmes d'information sont situés dans un ou plusieurs autres États membres, les autorités compétentes des États membres concernés coopèrent et se prêtent mutuellement assistance si nécessaire. Cette coopération suppose, au minimum : a) que les autorités compétentes appliquant des mesures de supervision ou d'exécution dans un État membre informent et consultent, par l'intermédiaire du point de contact unique, les autorités compétentes des autres États membres concernés en ce qui concerne les mesures de supervision et d'exécution prises ; b) qu'une autorité compétente puisse demander à une autre autorité compétente de	Norme de niveau législatif, qui sera à décliner par un décret.	Cf. Fiche d'impact « Notification d'incidents et partage d'informations ».

concourant aux missions de sécurité ou de défense des systèmes d'information. Les modalités d'application du présent article, notamment les modalités du partage d'informations, sont déterminées par décret en Conseil d'Etat.	prendre des mesures de supervision ou d'exécution ; c) qu'une autorité compétente, dès réception d'une demande motivée d'une autre autorité compétente, fournisse à l'autre autorité compétente une assistance mutuelle proportionnée à ses propres ressources afin que les mesures de supervision ou d'exécution puissent être mises en œuvre de manière effective, efficace et cohérente. L'assistance mutuelle visée au premier alinéa, point c), peut porter sur des demandes d'informations et des mesures de contrôle, y compris des demandes de procéder à des inspections sur place, à des contrôles à distance ou à des audits de sécurité ciblés. Une autorité compétente à laquelle une demande d'assistance est adressée ne peut refuser cette demande que s'il est établi que l'autorité n'est pas compétente pour fournir l'assistance demandée, que l'assistance demandée n'est pas proportionnée aux tâches de supervision de l'autorité compétente ou que la demande concerne des informations ou implique des activités dont la divulgation ou l'exercice seraient contraires aux intérêts essentiels de la sécurité nationale, la sécurité publique ou la défense de cet État membre. Avant de refuser une telle demande, l'autorité compétente consulte les autres autorités compétentes concernées ainsi que,		

	à la demande de l'un des États membres concernés, la Commission et l'ENISA.		
Art. 23 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'autorité nationale de sécurité des systèmes d'information, et, d'autre part, la Commission nationale de l'informatique et des libertés 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 Etats membres de l'Union européenne ou des centres de réponse aux incidents de sécurité informatique ou des organismes internationaux concourant aux missions de sécurité ou de défense des systèmes d'information. Les modalités d'application du présent article, notamment les modalités du partage d'informations,	Art. 37, 2. Le cas échéant et d'un commun accord, les autorités compétentes de différents États membres peuvent mener à bien des actions communes de supervision.	Norme de niveau législatif, qui sera à décliner par un décret.	Cf. Fiche d'impact « Notification d'incidents et partage d'informations ».

sont déterminées par décret en Conseil d'Etat.			
N/A	Art. 38, 1. Le pouvoir d'adopter des actes délégués conféré à la Commission est soumis aux conditions fixées au présent article.		
N/A	Art. 38, 2. Le pouvoir d'adopter des actes délégués visé à l'article 24, paragraphe 2, est conféré à la Commission pour une période de cinq ans à compter du 16 janvier 2023.		
N/A	Art. 38, 3. La délégation de pouvoir visée à l'article 24, paragraphe 2, peut être révoquée à tout moment par le Parlement européen ou le Conseil. La décision de révocation met fin à la délégation de pouvoir qui y est précisée. La révocation prend effet le jour suivant celui de la publication de ladite décision au *Journal officiel de l'Union européenne* ou à une date ultérieure qui est précisée dans ladite décision. Elle ne porte pas atteinte à la validité des actes délégués déjà en vigueur.		
N/A	Art. 38, 4.		

	Avant l'adoption d'un acte délégué, la Commission consulte les experts désignés par chaque État membre, conformément aux principes définis dans l'accord interinstitutionnel du 13 avril 2016 «Mieux légiférer».		
N/A	Art. 38, 5. Aussitôt qu'elle adopte un acte délégué, la Commission le notifie au Parlement européen et au Conseil simultanément.		
N/A	Art. 38, 6. Un acte délégué adopté en vertu de l'article 24, paragraphe 2, n'entre en vigueur que si le Parlement européen ou le Conseil n'a pas exprimé d'objections dans un délai de deux mois à compter de la notification de cet acte au Parlement européen et au Conseil ou si, avant l'expiration de ce délai, le Parlement européen et le Conseil ont tous deux informé la Commission de leur intention de ne pas exprimer d'objections. Ce délai est prolongé de deux mois à l'initiative du Parlement européen ou du Conseil.		
N/A	Art. 39, 1. La Commission est assistée par un comité. Ledit		

	comité est un comité au sens du règlement (UE) n° 182/2011.		
N/A	Art. 39, 2. Lorsqu'il est fait référence au présent paragraphe, l'article 5 du règlement (UE) n° 182/2011 s'applique.		
N/A	Art. 39, 3. Lorsque l'avis du comité doit être obtenu par procédure écrite, ladite procédure est close sans résultat lorsque, dans le délai prévu pour émettre un avis, le président du comité le décide ou un membre du comité le demande.		
N/A	Art. 40. Au plus tard le 17 octobre 2027 et tous les 36 mois par la suite, la Commission réexamine le fonctionnement de la présente directive et en fait rapport au Parlement européen et au Conseil. Le rapport évalue notamment la pertinence de la taille des entités concernées et des secteurs, sous-secteurs et types d'entité visés aux annexes I et II pour le fonctionnement de l'économie et de la société en ce qui concerne la cybersécurité. À cette fin et en vue de faire progresser la coopération		

	stratégique et opérationnelle, la Commission tient compte des rapports du groupe de coopération et du réseau des CSIRT sur l'expérience acquise au niveau stratégique et opérationnel. Le rapport est accompagné, si nécessaire, d'une proposition législative.		
N/A	Art. 41, 1. Les États membres adoptent et publient, au plus tard le 17 octobre 2024, les dispositions nécessaires pour se conformer à la présente directive. Ils en informent immédiatement la Commission. Ils appliquent ces dispositions à partir du 18 octobre 2024.		
N/A	Art. 41, 2. Lorsque les États membres adoptent les dispositions visées au paragraphe 1, celles-ci contiennent une référence à la présente directive ou sont accompagnées d'une telle référence lors de leur publication officielle. Les modalités de cette référence sont arrêtées par les États membres.		
N/A	Art. 42. Dans le règlement (UE) nº 910/2014, l'article 19		

	est supprimé avec effet au 18 octobre 2024.		
N/A	Art. 43. Dans la directive (UE) 2018/1972, les articles 40 et 41 sont supprimés avec effet au 18 octobre 2024.		
N/A	Art. 44. La directive (UE) 2016/1148 est abrogée avec effet au 18 octobre 2024. Les références à la directive abrogée s'entendent comme faites à la présente directive et sont à lire selon le tableau de correspondance figurant à l'annexe III.		
N/A	Art. 45 La présente directive entre en vigueur le vingtième jour suivant celui de sa publication au *Journal officiel de l'Union européenne*.		
N/A	Art. 46. Les États membres sont destinataires de la présente directive.		

ANNEXE III – TABLEAUX DE TRANSPOSITION DE LA DIRECTIVE (UE) 2022/2556 DU PARLEMENT EUROPEEN ET DU CONSEIL DU 14 DECEMBRE 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 RESILIENCE OPERATIONNELLE NUMERIQUE DU SECTEUR FINANCIER (DITE DIRECTIVE DORA)

Article 43 – Modification de la définition des prestataires de services techniques a l'appui de la fourniture de services de paiement

Dispositions de la directive à transposer	Normes de droit interne existantes portant déjà transposition de certaines dispositions de la directives	Nature juridique des nouvelles normes à adopter pour assurer l'entière transposition de la directive	Dispositions proposées	Observations
Article 7 (1) de la directive (UE) 2022/2556 du Parlement	7° du III de l'article L. 314-1 du code monétaire et	Norme de nature législative	Modification du 7° du III de l'article L. 314-1 du code	

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	financier		monétaire et financier	

Article 44 - Maintien de la résilience opérationnelle des gestionnaires de plateformes de négociation

Dispositions de la directive à transposer	Normes de droit interne existantes portant déjà transposition de certaines dispositions de la directives	Nature juridique des nouvelles normes à adopter pour assurer l'entière transposition de la directive	Dispositions proposées	Observations
Article 6 (4) de la 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,	I et III de l'article L. 420-3 du code monétaire et financier	Norme de nature législative	Modification du I et du III de l'article L. 420-3 du code monétaire et financier	

2014/65/UE, (UE) 2015/2366 et (UE) 2016/2341 en ce qui concerne la résilience opérationnelle numérique du secteur financier				

Article 45 - Gestion du risque lié aux technologies de l'information et de la communication par les entreprises de marché

Dispositions de la directive à transposer	Normes de droit interne existantes portant déjà transposition de certaines dispositions de la directives	Nature juridique des nouvelles normes à adopter pour assurer l'entière transposition de la directive	Dispositions proposées	Observations
Article 6 (3) de la 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,	I et III de l'article L. 421-11 du code monétaire et financier	Norme de nature législative	Modification du I et du III de l'article L. 421-11 du code monétaire et financier	

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 46 - Références aux risques liés aux technologies de l'information et de la communication au sein des dispositifs de gestion des risques des établissements de crédit et des sociétés de financement

Dispositions de la directive à transposer	Normes de droit interne existantes portant déjà transposition de certaines dispositions de la directives	Nature juridique des nouvelles normes à adopter pour assurer l'entière transposition de la directive	Dispositions proposées	Observations
Articles 4 (3) et 4(4) de la directive (UE) 2022/2556 du Parlement européen et du Conseil du 14 décembre 2022 modifiant les	Article L. 511-41-1-B du code monétaire et financier	Norme de nature législative	Modification du deuxième et du cinquième alinéa de l'article L. 511-41-1-B du code monétaire et financier. Modification de	

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			l'article L. 712-7 du code monétaire et financier réalisée par l'article 46 du projet de loi rend applicable le règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier à Saint-Pierre et Miquelon, en Nouvelle-Calédonie, en Polynésie française et dans les îles Wallis et Futuna qui sont des pays et	

			territoires d'outre-mer où le droit de l'Union européenne ne s'applique pas. Par coordination, l'article L. 771-1 est complété par les références au règlement (UE) 2022/2554 précité.	

Article 47 - Référence aux réseaux et systèmes d'information au sein des exigences de contrôle interne des établissements de crédit et des sociétés de financement

Dispositions de la directive à transposer	Normes de droit interne existantes portant déjà transposition de certaines dispositions de la	Nature juridique des nouvelles normes à adopter pour assurer l'entière transposition de la	Dispositions proposées	Observations

	directives	**directive**		
Article 4 (2) de la 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 L. 511-55 du code monétaire et financier	Norme de nature législative	Modification du premier alinéa de l'article L. 511-55 du code monétaire et financier. Modification de l'article L. 712-7 du code monétaire et financier réalisée par l'article 46 du projet de loi rend applicable le règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du	

			secteur financier à Saint-Pierre et Miquelon, en Nouvelle-Calédonie, en Polynésie française et dans les îles Wallis et Futuna qui sont des pays et territoires d'outre-mer où le droit de l'Union européenne ne s'applique pas. Par coordination, l'article L. 771-1 est complété par les références au règlement (UE) 2022/2554 précité.	

Article 48 – Obligation pour les prestataires de services de paiement de se conformer aux exigences du chapitre II du règlement DORA

Dispositions de la directive à transposer	Normes de droit interne existantes portant déjà transposition de certaines dispositions de la directives	Nature juridique des nouvelles normes à adopter pour assurer l'entière transposition de la directive	Dispositions proposées	Observations
Article 7 (1) de la 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,	Article L. 521-9 du code monétaire et financier	Norme de nature législative	Modification de l'article L. 521-9 du code monétaire et financier en ajoutant un alinéa avec renvoi au chapitre II du règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14	

2014/59/UE, 2014/65/UE, (UE) 2015/2366 et (UE) 2016/2341 en ce qui concerne la résilience opérationnelle numérique du secteur financier			décembre 2022 sur la résilience opérationnelle numérique du secteur financier.	

Article 49 – Modification de la liste des prestataires de services de paiement soumis aux obligations de notification des incidents opérationnels et de sécurité majeurs

Dispositions de la directive à transposer	Normes de droit interne existantes portant déjà transposition de certaines dispositions de la directives	Nature juridique des nouvelles normes à adopter pour assurer l'entière transposition de la directive	Dispositions proposées	Observations
Article 7 (5) de la 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,	Article L. 521-10 du code monétaire et financier (I et II)	Norme de nature législative	Modification du II de l'article L. 521-10 du code monétaire et financier	

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 50 - Référence aux réseaux et systèmes d'information au sein des exigences de contrôle et de sauvegarde des prestataires de service d'investissement

Dispositions de la directive à transposer	Normes de droit interne existantes portant déjà transposition de certaines dispositions de la directives	Nature juridique des nouvelles normes à adopter pour assurer l'entière transposition de la directive	Dispositions proposées	Observations
Article 4 (2) de la 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,	Article L. 533-2 du code monétaire et financier	Norme de nature législative	Modification du premier alinéa de l'article L. 533-2 du code monétaire et financier. Modification de l'article L. 712-7 du code monétaire et financier réalisée par l'article 46 du	

2014/59/UE, 2014/65/UE, (UE) 2015/2366 et (UE) 2016/2341 en ce qui concerne la résilience opérationnelle numérique du secteur financier			projet de loi rend applicable le règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier à Saint-Pierre et Miquelon, en Nouvelle-Calédonie, en Polynésie française et dans les îles Wallis et Futuna qui sont des pays et territoires d'outre-mer où le droit de l'Union européenne ne	

			s’applique pas. Par coordination, l’article L. 771-1 est complété par les références au règlement (UE) 2022/2554 précité.	

Article 51 - Systèmes de technologies de l'information et de la communication (TIC) et dispositifs de contrôle des prestataires de services d'investissement

Dispositions de la directive à transposer	Normes de droit interne existantes portant déjà transposition de certaines dispositions de la directives	Nature juridique des nouvelles normes à adopter pour assurer l'entière transposition de la directive	Dispositions proposées	Observations
Articles 1 (1) et 6 (1) de la directive (UE) 2022/2556 du Parlement européen et du Conseil du 14 décembre 2022 modifiant les directives 2009/65/CE, 2009/138/CE,	Article L. 533-10 du code monétaire et financier	Norme de nature législative	Modification du I. et du II. de l'article L. 533-10 du code monétaire et financier.	

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 52 - Systèmes de contrôle des risques mis en œuvre par les prestataires de services d'investissement autres que les sociétés de gestion de portefeuille qui ont recours à la négociation algorithmique

Dispositions de la directive à transposer	Normes de droit interne existantes portant déjà transposition de certaines dispositions de la directives	Nature juridique des nouvelles normes à adopter pour assurer l'entière transposition de la directive	Dispositions proposées	Observations
Article 6 (2) de la 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,	Article L. 533-10-4 du code monétaire et financier	Norme de nature législative	Modification du 1° et du 2° Ide l'article L. 533-10-4 du code monétaire et financier.	

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 53 - Référence aux prestataires informatiques critiques au sein des tiers auxquels l'Autorité de contrôle prudentiel et de résolution peut demander toute information

Dispositions de la directive à transposer	Normes de droit interne existantes portant déjà transposition de certaines dispositions de la directives	Nature juridique des nouvelles normes à adopter pour assurer l'entière transposition de la directive	Dispositions proposées	Observations
Article 4 (1) de la 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,	Article L. 612-24 du code monétaire et financier	Norme de nature législative	Modification du troisième alinéa de l'article L. 612-24 du code monétaire et financier. Modification de l'article L. 712-7 du code monétaire et financier réalisée par l'article 46 du	

2014/59/UE, 2014/65/UE, (UE) 2015/2366 et (UE) 2016/2341 en ce qui concerne la résilience opérationnelle numérique du secteur financier			projet de loi rend applicable le règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier à Saint-Pierre et Miquelon, en Nouvelle-Calédonie, en Polynésie française et dans les îles Wallis et Futuna qui sont des pays et territoires d'outre-mer où le droit de l'Union européenne ne	

			s’applique pas. Par coordination, l’article L. 781-1 est complété par les références au règlement (UE) 2022/2554 précité.	

Article 54 - Référence à la résilience opérationnelle numérique au sein des plans préventifs de résolution des établissements de crédit et des sociétés de financement

Dispositions de la directive à transposer	Normes de droit interne existantes portant déjà transposition de certaines dispositions de la directives	Nature juridique des nouvelles normes à adopter pour assurer l'entière transposition de la directive	Dispositions proposées	Observations
Points a et b du 1 de l'Article 5 de la 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,	3° et 17° du III de l'article L. 613-38 du code monétaire et financier	Norme de nature législative	Modification des 3° et 17° du III de l'article L. 613-38 du code monétaire et financier. Modification de l'article L. 712-7 du code monétaire et financier réalisée par l'article 46 du	

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			projet de loi rend applicable le règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier à Saint-Pierre et Miquelon, en Nouvelle-Calédonie, en Polynésie française et dans les îles Wallis et Futuna qui sont des pays et territoires d'outre-mer où le droit de l'Union européenne ne	

			s’applique pas. Par coordination, l’article L. 781-1 est complété par les références au règlement (UE) 2022/2554 précité.	

Article 55 – Modification de la liste des autorités habilitées à se communiquer des renseignements utiles à l'exercice de leurs fonctions

Dispositions de la directive à transposer	Normes de droit interne existantes portant déjà transposition de certaines dispositions de la directives	Nature juridique des nouvelles normes à adopter pour assurer l'entière transposition de la directive	Dispositions proposées	Observations
Article 49 (2) du règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE)	Article L. 631-1 du code monétaire et financier	Norme de nature législative	Modification du quatrième alinéa du II de l'article L. 631-1 du code monétaire et financier. Modification de l'article L. 712-7 du code monétaire et financier réalisée par l'article 46 du	

no 1060/2009, (UE) no 648/2012, (UE) no 600/2014, (UE) no 909/2014 et (UE) 2016/1011			projet de loi qui rend applicable le règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier à Saint-Pierre et Miquelon, en Nouvelle-Calédonie, en Polynésie française et dans les îles Wallis et Futuna qui sont des pays et territoires d'outre-mer où le droit de l'Union européenne ne	

			s’applique pas. Par coordination, l’article L. 781-1 est complété par les références au règlement (UE) 2022/2554 précité.	

Article 57 – Nouvelles obligations pour les entreprises d'assurance et de réassurance en matière de gouvernance des risques liés à l'utilisation des systèmes d'information

Dispositions de la directive à transposer	Normes de droit interne existantes portant déjà transposition de certaines dispositions de la directive	Nature juridique des nouvelles normes à adopter pour assurer l'entière transposition de la directive	Dispositions proposées	Observations
Articles 2 (1) et 8 de la 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,	Article L. 354-1 du code des assurances	Norme de nature législative	Modifications du troisième alinéa et du quatrième alinéa de l'article L. 354-1 du code des assurances	

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 58 – Extension aux groupes d'assurance des nouvelles obligations de gouvernance des risques liés à l'utilisation des systèmes d'information

Dispositions de la directive à transposer	Normes de droit interne existantes portant déjà transposition de certaines dispositions de la directive	Nature juridique des nouvelles normes à adopter pour assurer l'entière transposition de la directive	Dispositions proposées	Observations
Article 2 (1) de la 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,	Article L. 356-18 du code des assurances	Norme de nature législative	Modifications du troisième alinéa et du quatrième alinéa de l'article L. 356-18 du code des assurances	

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 59 – Nouvelles obligations pour les unions et mutuelles du code de la mutualité en matière de gouvernance des risques liés à l'utilisation des systèmes d'information

Dispositions de la directive à transposer	Normes de droit interne existantes portant déjà transposition de certaines dispositions de la directive	Nature juridique des nouvelles normes à adopter pour assurer l'entière transposition de la directive	Dispositions proposées	Observations
Article 2 (1) de la 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,	Article L. 211-12 du code de la mutualité	Norme de nature législative	Modification du quatrième alinéa de l'article L. 211-12 du code de la mutualité	

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 60 – Suppression de dispositions redondantes dans le code de la mutualité

Dispositions de la directive à transposer	Normes de droit interne existantes portant déjà transposition de certaines dispositions de la directive	Nature juridique des nouvelles normes à adopter pour assurer l'entière transposition de la directive	Dispositions proposées	Observations
Aucune (modification en opportunité)	Articles L. 211-12 et L. 212-1 du code de la mutualité	Norme de nature législative	Modification du deuxième alinéa de l'article L. 212-1 du code de la mutualité	

Article 61 – Nouvelles obligations pour les institutions de prévoyance et unions du code de la sécurité sociale en matière de gouvernance des risques liés à l'utilisation des systèmes d'information

Dispositions de la directive à transposer	Normes de droit interne existantes portant déjà transposition de certaines dispositions de la directive	Nature juridique des nouvelles normes à adopter pour assurer l'entière transposition de la directive	Dispositions proposées	Observations
Article 2 (1) de la 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,	Article L. 931-7 du code de la sécurité sociale	Norme de nature législative	Modification du quatrième alinéa de l'article L. 931-7 du code de la sécurité sociale	

2014/59/UE, 2014/65/UE, (UE) 2015/2366 et (UE) 2016/2341 en ce qui concerne la résilience opérationnelle numérique du secteur financier				

ANNEXE IV – TABLEAU SYNOPTIQUE DES OPTIONS LAISSEES PAR LA DIRECTIVE NIS 2

Option permise par la directive NIS 2	Choix dans la transposition
Art. 2, 5., a) : Les États membres peuvent prévoir que la présente directive s'applique : a) aux entités de l'administration publique au niveau local ;	La France a choisi d'inclure les collectivités locales dans le champ de la directive Référence dans le projet de loi : b) à g) du 7° de l'article 8 et 4° de l'article 9
Art. 3 : Les États membres peuvent mettre en place des mécanismes nationaux permettant aux entités de s'enregistrer elles-mêmes.	La France a choisi d'implémenter un service permettant aux entités importantes ou essentielles de se déclarer auprès de l'autorité national compétente et de fournir les informations demandées par la directive.
Art. 2, 5., b) : Les États membres peuvent prévoir que la présente directive s'applique : b) aux établissements d'enseignement, en particulier lorsqu'ils mènent des activités de recherche critiques.	La France a choisi d'activer cette option. En revanche, la France a choisi de la restreinte aux seuls établissements d'enseignement menant des activités de recherche. Ces établissements peuvent être entité importante ou essentielle. De plus, une décision du Premier ministre sur avis des ministères concernés pourra exclure certains de

	ces établissements des obligations prévues par le projet de loi. Référence dans le projet de loi : 10° de l'article 8 et 5° de l'article 9
Art. 8, 1. : Chaque État membre désigne ou établit une ou plusieurs autorités compétentes chargées de la cybersécurité et des tâches de supervision visées au chapitre VII (ci-après dénommées « autorités compétentes »).	La France a fait le choix de désigner une autorité nationale de sécurité des systèmes d'information cheffe de file, chargée de la mise en œuvre de la législation et de la politique du Gouvernement en matière de sécurité des systèmes d'information régie par le titre II et de son contrôle. Référence dans le projet de loi : article 5 Le renvoi à un décret permettra de préciser en quelles matières spécifiques certains ministères exerceront, dans le domaine de la défense, les compétences de l'autorité nationale de sécurité des systèmes d'information au sens de l'article 8 de la directive.
Art. 9, 1. : Chaque État membre désigne ou établit une ou plusieurs autorités compétentes qui sont chargées de la gestion des incidents de cybersécurité majeurs et des crises (ci-après dénommées « autorités de	La France a fait le choix de désigner une unique autorité de gestion des crises cyber au sens de la directive et d'en confier la responsabilité à l'autorité nationale de sécurité des systèmes

gestion des crises cyber »).	d'information. Sera traité au niveau réglementaire
Art. 10, 1. : Chaque État membre désigne ou met en place un ou plusieurs CSIRT. Les CSIRT peuvent être désignés ou établis au sein d'une autorité compétente.	La France a fait le choix de désigner un unique CSIRT (centre de réponse aux incidents de sécurité informatique) et d'en confier la responsabilité à l'autorité nationale de sécurité des systèmes d'information. Actuellement, cette responsabilité serait assumée par le CERT-FR établi au sein de l'ANSSI Sera traité au niveau réglementaire
Art. 21, 2. : Les mesures visées au paragraphe 1 sont fondées sur une approche «tous risques» qui vise à protéger les réseaux et les systèmes d'information ainsi que leur environnement physique contre les incidents, et **elles comprennent au moins**: a) les politiques relatives à l'analyse des risques et à la sécurité des systèmes d'information; b) la gestion des incidents; c) la continuité des activités, par exemple la gestion des sauvegardes et la reprise des activités, et la gestion des crises; d) 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 France prévoit au niveau réglementaire de : - détailler certaines mesures. Par exemple, le point e. de la directive sera détaillé pour prévoir des exigences sur le cloisonnement des systèmes d'information et la mise en œuvre de mesures techniques permettant de filtrer les communications depuis ou vers un système d'information aux seules communications strictement nécessaires aux activités ou services supportés par ledit système d'information. Pour les points b) et c), la France prévoit des exigences en

e) 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; f) des politiques et des procédures pour évaluer l'efficacité des mesures de gestion des risques en matière de cybersécurité; g) les pratiques de base en matière de cyberhygiène et la formation à la cybersécurité; h) des politiques et des procédures relatives à l'utilisation de la cryptographie et, le cas échéant, du chiffrement; i) la sécurité des ressources humaines, des politiques de contrôle d'accès et la gestion des actifs; j) 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.	matière d'exercice et d'entrainement pour obliger une entité importante ou essentielle à tester ces capacités de réponse à incident et de continuité d'activité. - d'ajouter certaines mesures. Par exemple, la France prévoit des mesures de protection des annuaires d'identité (par exemple : ActiveDirectory de Microsoft) au regard de la criticité de ces annuaires dans les activités ou services supportés par les systèmes d'information d'une entité importante ou essentielle.
Art. 32, 33 : Les résultats de tout audit de sécurité ciblé sont mis à la disposition de l'autorité compétente. Les coûts de cet audit de sécurité ciblé effectué par un organisme indépendant sont à la charge de l'entité contrôlée, sauf lorsque l'autorité compétente en décide autrement dans des cas dûment motivés.	La France a choisi de faire porter plus largement le coût des contrôles aux entités importantes et essentielles et pas uniquement les audits. Cette volonté est alignée sur la position actuelle ou les contrôles prévus dans NIS1 ou le volet cyber du dispositif de sécurité des activités d'importance vitale. <u>Référence dans le projet de loi :</u> article 29

Art. 32, 2. : Les États membres veillent à ce que les autorités compétentes, lorsqu'elles accomplissent leurs tâches de supervision à l'égard d'entités essentielles, aient le pouvoir de soumettre ces entités à, **au minimum**: a) des inspections sur place et des contrôles à distance, y compris des contrôles aléatoires effectués par des professionnels formés; b) des audits de sécurité réguliers et ciblés réalisés par un organisme indépendant ou une autorité compétente; c) des audits ad hoc, notamment lorsqu'ils sont justifiés en raison d'un incident important ou d'une violation de la présente directive par l'entité essentielle; d) des scans de sécurité fondés sur des critères d'évaluation des risques objectifs, non discriminatoires, équitables et transparents, si nécessaire avec la coopération de l'entité concernée; e) des demandes d'informations nécessaires à l'évaluation des mesures de gestion des risques en matière de cybersécurité adoptées par l'entité concernée, notamment les politiques de cybersécurité consignées par écrit, ainsi que du respect de l'obligation de soumettre des informations aux autorités compétentes conformément à l'article 27; f) des demandes d'accès à des données, à des documents et à toutes informations nécessaires à l'accomplissement de leurs tâches de supervision; g) des demandes de preuves de la mise en œuvre de politiques de cybersécurité, telles que les résultats des audits de sécurité effectués par un auditeur qualifié et les éléments de preuve sous-jacents correspondants.	La France a choisi de reprendre strictement les éléments de la directive sans aller au-delà <u>Référence dans le projet de loi :</u> articles 27 et 29

Art. 32, 4. | Art. 33, 4. : Les États membres veillent à ce que leurs autorités compétentes, lorsqu'elles exercent leurs pouvoirs d'exécution à l'égard d'entités essentielles, **aient au minimum le pouvoir**: a) d'émettre des avertissements concernant les violations de la présente directive par les entités concernées; b) 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 présente directive; c) d'ordonner aux entités concernées de mettre un terme à un comportement qui viole la présente directive et de ne pas le réitérer; d) 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; e) 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; f) d'ordonner aux entités concernées de mettre en œuvre les recommandations formulées à la suite d'un audit de sécurité dans un délai	La France a choisi de reprendre strictement les éléments de la directive sans aller au-delà Référence dans le projet de loi : articles 31 et 32

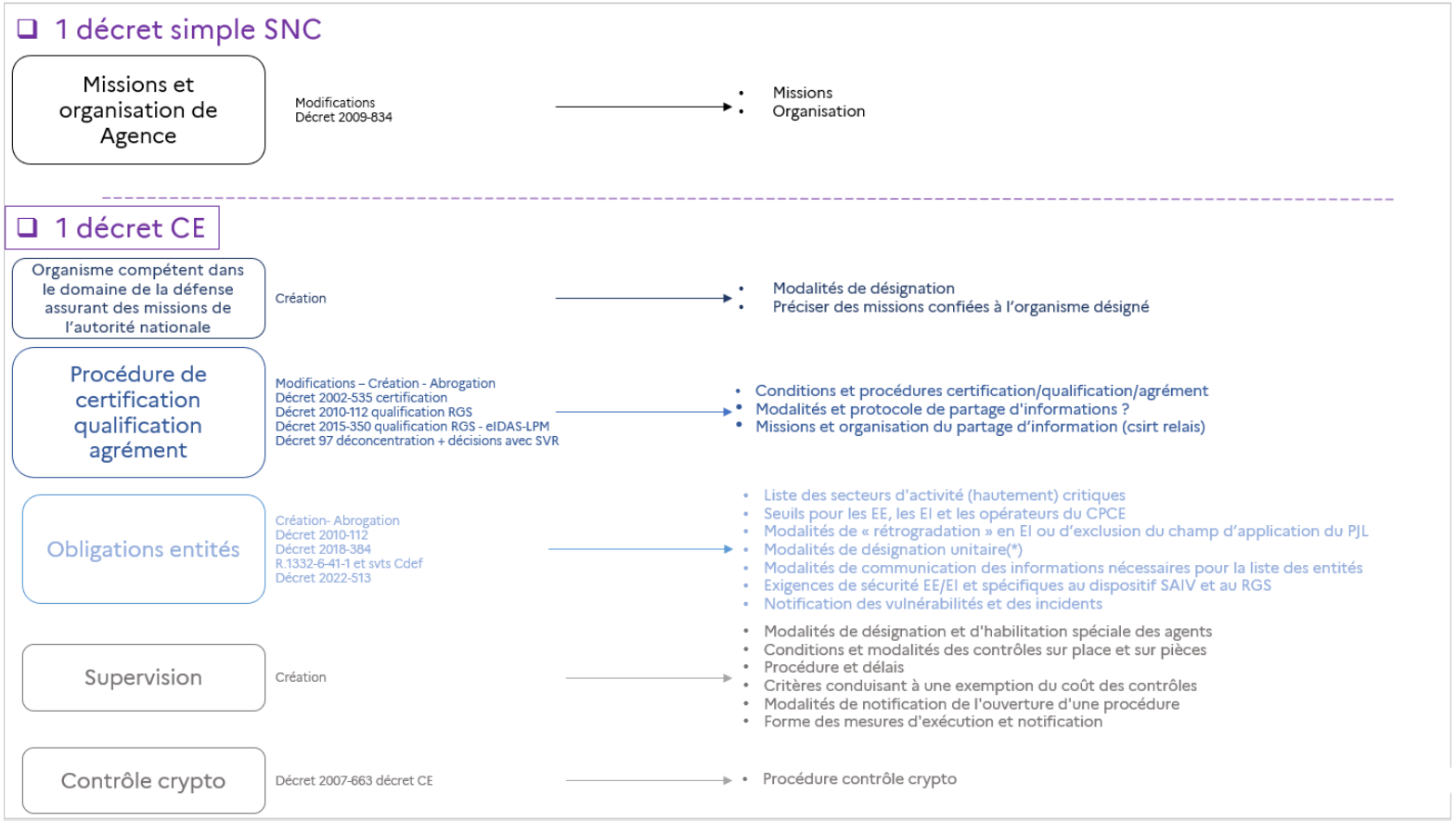
raisonnable; g) de désigner, pour une période déterminée, un responsable du contrôle ayant des tâches bien définies pour superviser le respect, par les entités concernées, des articles 21 et 23; h) d'ordonner aux entités concernées de rendre publics les aspects de violations de la présente directive de manière spécifique; i) d'imposer ou de demander aux organes compétents ou aux juridictions d'imposer, conformément au droit national, une amende administrative en vertu de l'article 34 en plus de l'une ou l'autre des mesures visées aux points a) à h) du présent paragraphe.	
Art. 34, 4. et 5. : Les États membres veillent à ce que, lorsqu'elles violent l'article 21 ou 23, les entités essentielles soient soumises, conformément aux paragraphes 2 et 3 du présent article, à des amendes administratives d'un montant maximal **s'élevant à au moins 10 000 000 EUR 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 États membres veillent à ce que, lorsqu'elles violent l'article 21 ou 23, les entités importantes soient soumises, conformément aux paragraphes 2 et 3 du présent article, à des amendes administratives d'un montant maximal **s'élevant à au moins 7 000 000 EUR 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	La France a choisi d'aligner le montant des sanctions sur ceux prévus par la directive. Référence dans le projet de loi : article 37

élevé étant retenu.	

PREMIER MINISTRE

Liberté
Égalité
Fraternité

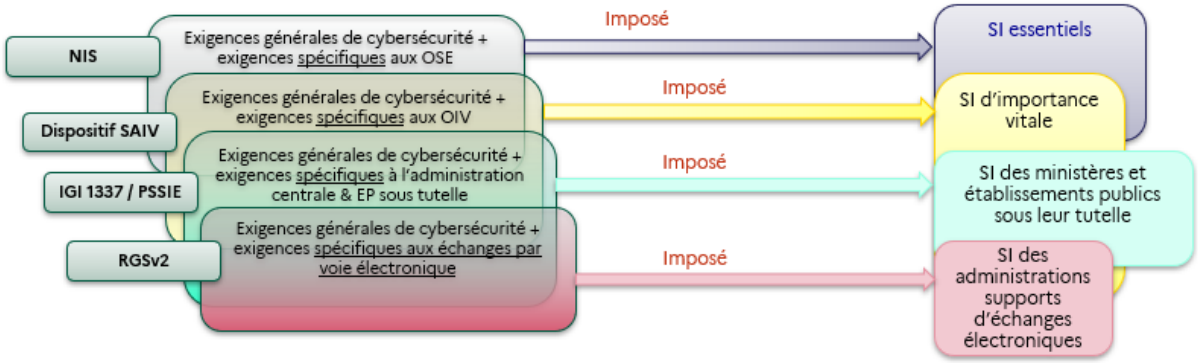
ANNEXE V – TEXTES REGLEMENTAIRES PREVUS POUR LE TITRE II



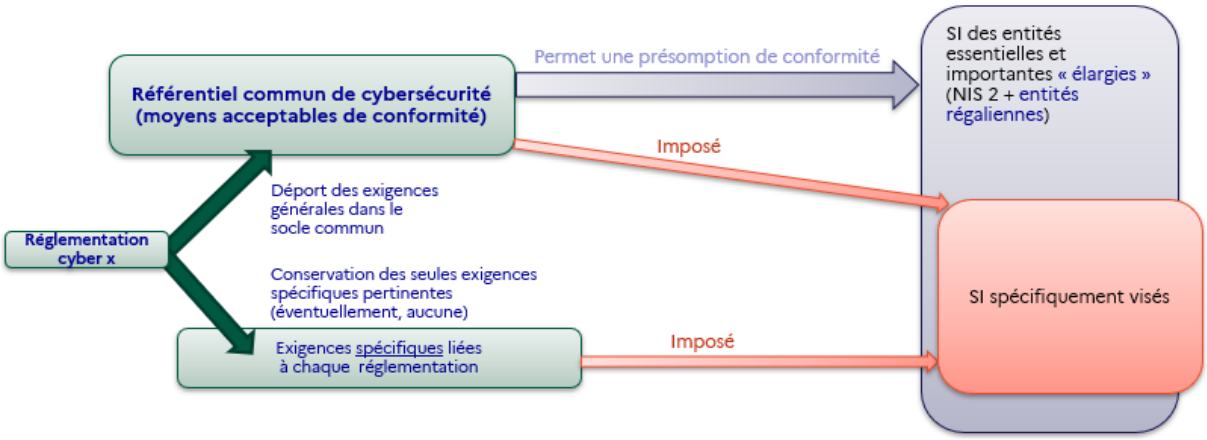
PREMIER MINISTRE
Liberté
Égalité
Fraternité

ANNEXE VI – SCHEMA EXPLICATIF DE LA STRATEGIE DE SIMPLIFICATION REGLEMENTAIRE

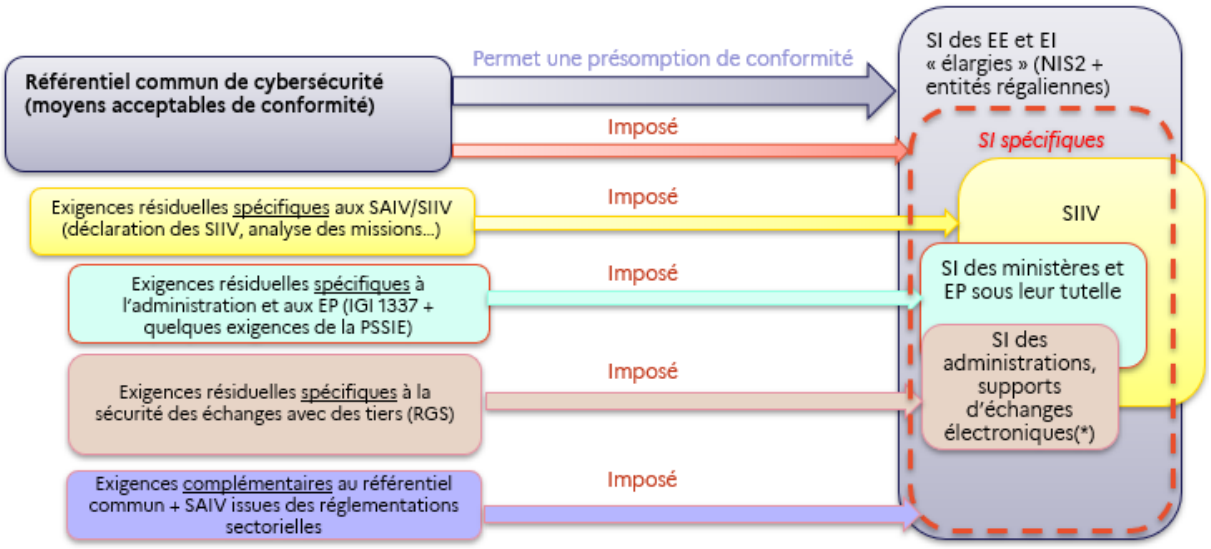
Problématique : Des exigences de nature similaire, mais avec des logiques de rédaction et spécificités de fond différentes en fonction des cadres réglementaires



Objectif : Faire des règles NIS 2 le « socle » transverse permettant d'assurer la protection des opérateurs contre la menace cybercriminelle de masse



Enjeu : Etendre l'application de NIS 2 et préserver l'efficacité de chaque dispositif complémentaire de NIS


Référentiel commun de cybersécurité (moyens acceptables de conformité)
Permet une présomption de conformité
Imposé
Exigences résiduelles spécifiques aux SAIV/SIIV (déclaration des SIIV, analyse des missions…)
Imposé
Exigences résiduelles spécifiques à l'administration et aux EP (IGI 1337 + quelques exigences de la PSSIE)
Imposé
Exigences résiduelles spécifiques à la sécurité des échanges avec des tiers (RGS)
Imposé
Exigences complémentaires au référentiel commun + SAIV issues des réglementations sectorielles
Imposé
SI des EE et EI « élargies » (NIS2 + entités régaliennes)
SI spécifiques
SIIV
SI des ministères et EP sous leur tutelle
SI des administrations, supports d'échanges électroniques(*)