N° 1779

ASSEMBLÉE NATIONALE

CONSTITUTION DU 4 OCTOBRE 1958

DIX-SEPTIÈME LÉGISLATURE

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

TEXTE DE LA COMMISSION SPÉCIALE

ANNEXE AU RAPPORT

PROJET DE LOI

relative à la **résilience** *des* **infrastructures critiques** *et au* **renforcement** *de la* **cybersécurité**

(Première lecture)

(Procédure accélérée)

Voir les numéros :
Sénat : **33, 393, 394** et **T.A. 78** (2024-2025).
Assemblée nationale : **1112**.

TITRE IER

RÉSILIENCE DES ACTIVITÉS D'IMPORTANCE VITALE

CHAPITRE IER

Dispositions générales

Article 1er

① Le chapitre II du titre III du livre III de la première partie du code de la défense est ainsi rédigé :

② *« CHAPITRE II*

③ ***« Résilience des activités d'importance vitale***

④ *« Section 1*

⑤ ***« Dispositions générales relatives aux activités d'importance vitale***

⑥ « *Art. L. 1332-1.* – Pour l'application du présent chapitre, on entend par :

⑦ « 1° Activités d'importance vitale : les activités indispensables au fonctionnement de l'économie ou de la société ainsi qu'à la défense ou à la sécurité de la Nation ;

⑧ « 2° Infrastructure critique : tout ou partie d'un bien, d'une installation, d'un équipement, d'un réseau ou d'un système nécessaire à l'exercice d'une activité d'importance vitale ou dont une perturbation pourrait mettre gravement en cause la santé de la population ou l'environnement ;

⑨ « Parmi les infrastructures critiques, sont distingués :

⑩ « *a)* Les points d'importance vitale, c'est-à-dire les installations les plus sensibles, notamment celles qui sont difficilement substituables ;

⑪ « *b)* 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, à l'utilisation ou à la protection d'une ou de plusieurs infrastructures critiques ;

⑫ « 3° Incident : un événement qui perturbe ou est susceptible de perturber de manière importante l'exercice d'une activité d'importance vitale ;

⑬ « 4° Résilience : la capacité d'un opérateur à prévenir tout type d'incident, à s'en protéger et à y résister, afin d'assurer la continuité de la ou des activités d'importance vitale qu'il exerce.

⑭ « *Art. L. 1332-2. – (Non modifié)* I. – Sont désignés opérateurs d'importance vitale par l'autorité administrative :

⑮ « 1° Les opérateurs publics ou privés exerçant, au moyen d'une ou de plusieurs infrastructures critiques situées sur le territoire national, une activité d'importance vitale.

⑯ « 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, justifient que cet opérateur soit regardé comme une entité critique au sens de cette directive ;

⑰ « 2° Les opérateurs publics ou privés, les gestionnaires, les propriétaires ou les 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 de plusieurs installations de ces établissements peut présenter un danger d'une particulière gravité pour la population ou l'environnement.

⑱ « II. – Ces opérateurs mettent en œuvre, à leurs frais, les obligations leur incombant prévues au présent chapitre.

⑲ « Lorsqu'un opérateur d'importance vitale exerce une activité d'importance vitale ou gère une infrastructure critique pour le compte d'une personne publique, cette dernière en est informée par l'autorité administrative.

⑳ *« Sous-section 1*

㉑ *« Dispositions applicables aux opérateurs d'importance vitale*

㉒ « *Art. L. 1332-3. – (Non modifié)* 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 sécurité de leurs infrastructures critiques, notamment des points d'importance vitale désignés par l'autorité administrative.

㉓ « Cette analyse est réalisée dans un délai de neuf mois à compter de la désignation prévue au I de l'article L. 1332-2 et est réévaluée au moins tous les quatre ans.

㉔ « Sur le fondement de cette analyse, les opérateurs d'importance vitale adoptent des mesures proportionnées de résilience, techniques, opérationnelles et organisationnelles, afin d'assurer la continuité des activités d'importance vitale qu'ils exercent et de sauvegarder leurs infrastructures critiques.

㉕ « L'analyse des risques ainsi que les mesures de résilience sont détaillées dans un document dénommé "plan de résilience opérateur" élaboré par l'opérateur, dans un délai de dix mois à compter de la désignation prévue au même I, et approuvé par l'autorité administrative.

㉖ « Lorsque, en application d'accords internationaux 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 troisième alinéa du présent article, l'autorité administrative peut décider que ce document tient lieu, pour tout ou partie, du "plan de résilience opérateur".

㉗ « 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 met en demeure l'opérateur de le réaliser, de le modifier ou de le mettre en œuvre dans un délai qu'elle fixe et qui ne peut être inférieur à un mois.

㉘ « L'autorité administrative peut assortir cette mise en demeure d'une astreinte d'un montant maximal de 5 000 euros par jour de retard à compter de l'expiration du délai imparti par la mise en demeure.

㉙ « 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.

(30) « 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 I^er^ et du chapitre III du titre IX du livre V du code de l'environnement.

(31) « Un décret en Conseil d'État précise 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 code.

(32) « *Art. L. 1332-4.* – Les opérateurs d'importance vitale réalisent, 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 et de leurs sous-traitants. L'analyse des dépendances à l'égard des sous-traitants est réalisée dans un délai fixé par voie réglementaire. Les mesures de résilience adoptées par les opérateurs d'importance vitale tiennent compte de cette analyse. Cette analyse évalue spécifiquement les risques liés à la dépendance envers des fournisseurs de solutions logicielles et matérielles propriétaires, notamment en termes de continuité de service, de coût à long terme et de capacité d'audit indépendant.

(33) « Les opérateurs d'importance vitale prennent les mesures nécessaires pour garantir l'application du présent chapitre.

(34) « *Art. L. 1332-5.* – Chaque opérateur pour lequel un ou plusieurs points d'importance vitale sont désignés en application du présent chapitre réalise pour chacun d'eux un document dénommé "plan particulier de résilience" détaillant les mesures de protection et de résilience le concernant.

(35) « Ces mesures comportent notamment des dispositifs et des dispositions efficaces de surveillance, d'alarme, de protection matérielle et de conditions d'accès. Le plan est approuvé par l'autorité administrative.

(36) « 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".

(37) « En cas de refus de l'opérateur d'élaborer ce plan, de le modifier afin de le rendre conforme aux exigences prévues aux trois premiers alinéas ou de le mettre en œuvre, l'autorité administrative met en demeure l'opérateur

de le réaliser, de le modifier ou de le mettre en œuvre dans un délai qu'elle fixe et qui ne peut être inférieur à un mois.

(38) « L'autorité administrative peut assortir cette mise en demeure d'une astreinte d'un montant maximal de 5 000 euros par jour de retard à compter de l'expiration du délai imparti par la mise en demeure.

(39) « 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.

(40) « *Art. L. 1332-6.* – Avant d'accorder une autorisation d'accès physique ou à distance à ses infrastructures critiques, 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, l'opérateur d'importance vitale peut demander l'avis de l'autorité administrative compétente à la suite d'une enquête administrative conduite dans les conditions prévues à l'article L. 114-1 du code de la sécurité intérieure, selon des modalités fixées par un décret en Conseil d'État pris après avis de la Commission nationale de l'informatique et des libertés.

(41) « 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 infrastructures critiques ou qui implique l'occupation de fonctions sensibles.

(42) « 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 énumérées par l'opérateur dans le plan de résilience prévu au quatrième alinéa de l'article L. 1332-3 du présent code en tenant compte, le cas échéant, de critères déterminés par l'autorité administrative en fonction du secteur d'activité de l'opérateur.

(43) « Les cas dans lesquels les accès physiques ou à distance peuvent justifier la demande d'avis sont précisés par l'opérateur dans le plan de résilience prévu au même quatrième alinéa et, le cas échéant, dans le plan particulier de résilience prévu à l'article L. 1332-5 en tenant compte des vulnérabilités à des actes de malveillance.

(44) « La personne concernée est informée de l'enquête administrative dont elle fait l'objet.

(45) « 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.

(46) « *Art. L. 1332-7. – (Non modifié)* Les opérateurs d'importance vitale désignés au titre du 1° du I de l'article L. 1332-2 notifient à l'autorité administrative, au plus tard vingt-quatre heures après en avoir pris connaissance, tout incident susceptible de compromettre la continuité de leurs activités d'importance vitale, dans des conditions fixées par décret en Conseil d'État.

(47) « L'autorité administrative informe le public de cet incident lorsqu'elle estime qu'il est dans l'intérêt général de le faire.

(48) *« Sous-section 2*

(49) *« Dispositions applicables aux entités critiques d'importance européenne particulière*

(50) « *Art. L. 1332-8.* – Les opérateurs d'importance vitale qui fournissent les services essentiels ou des services essentiels similaires à ou dans au moins six États membres en informent l'autorité administrative au plus tard en même temps que la présentation pour approbation du plan de résilience prévu au quatrième alinéa de l'article L. 1332-3.

(51) « Ces opérateurs sont identifiés comme entités critiques d'importance européenne particulière dans les conditions prévues à l'article 17 de la 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.

(52) « 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 domaines peuvent être dispensés 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'État.

(53) « *Art. L. 1332-9. – (Non modifié)* Lorsque l'opérateur a été désigné par la Commission européenne comme entité critique d'importance européenne

particulière, il peut, sur demande motivée de la Commission européenne ou d'un ou de plusieurs des États membres auxquels ou dans lesquels le service essentiel est fourni et 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, aux systèmes et aux installations relatifs à la fourniture de ses services essentiels qui sont nécessaires à l'exécution de cette mission de conseil, dans le respect des secrets protégés par la loi.

(54) « 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 peuvent être prises pour améliorer sa résilience.

(55) *« Sous-section 3*

(56) *« Dispositifs techniques concourant à la protection des installations d'importance vitale*

(57) « *Art. L. 1332-10. – (Non modifié)* À des fins de protection des établissements, des installations et des ouvrages d'importance vitale mentionnés au I de l'article L. 1332-2, les services de l'État concourant à la défense nationale, à la sûreté de l'État et à la sécurité intérieure peuvent procéder, au moyen de caméras installées sur des aéronefs, à la captation, à l'enregistrement et à la transmission d'images dans les conditions définies aux articles L. 2364-2 à L. 2364-4.

(58) *« Sous-section 4*

(59) *« Dispositions applicables aux systèmes d'information*

(60) « *Art. 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 fourniture de leurs services, les opérateurs d'importance vitale mettent en œuvre les obligations prévues aux articles 14 à 16 et 17 de la loi n° du relative à la résilience des infrastructures critiques et au renforcement de la cybersécurité.

(61) « Les opérateurs d'importance vitale ne sont pas tenus de mettre en œuvre les obligations prévues aux articles 14 et 15 de la **même** loi lorsqu'ils sont soumis, en application d'un acte juridique de l'Union européenne, à des exigences sectorielles de sécurité des réseaux et des systèmes d'information qu'ils utilisent dans le cadre de leurs activités ou de la fourniture de leurs services ayant un effet au moins équivalent.

⑫ « II. – 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 au I de l'article L. 1332-2 du présent code doivent mettre en œuvre.

⑬ *« Section 2*

⑭ ***« Contrôles et sanctions administratives***

⑮ *« Sous-section 1*

⑯ *« Habilitation et contrôles*

⑰ « *Art. L. 1332-12. – (Non modifié)* Sont habilités à rechercher et à constater les 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'État spécialement désignés et assermentés à cette fin dans des conditions précisées par décret en Conseil d'État.

⑱ « *Art. L. 1332-13. – (Non modifié)* 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 services.

⑲ « Ils peuvent accéder à tout document nécessaire à l'accomplissement de leur mission auprès des administrations publiques, des établissements et des organismes placés sous le contrôle de l'État et des collectivités territoriales ainsi que dans les entreprises ou les services concédés par l'État, les régions, les départements et les communes.

⑳ « Ils peuvent recueillir, sur place ou sur convocation, tout renseignement, toute justification ou tout document nécessaire aux contrôles. À ce titre, ils peuvent exiger la communication de documents de toute nature propres à faciliter l'accomplissement de leur mission. 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.

㉑ « 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.

⑫ « Ils sont astreints au secret professionnel pour les faits, les actes ou les 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.

⑬ « Les manquements sont constatés par des procès-verbaux, qui font foi jusqu'à preuve contraire. Il est dressé procès-verbal des vérifications et des visites menées en application du présent article.

⑭ « *Art. L. 1332-14. – (Non modifié)* 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.

⑮ « 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 à 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.

⑯ « Le présent article ne s'applique pas à l'État et à ses établissements publics administratifs qui font l'objet d'un contrôle.

⑰ *« Sous-section 2*

⑱ *« Sanctions*

⑲ « *Art. L. 1332-15. – (Non modifié)* Tout manquement au 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.

⑳ « 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.

(81) « La commission des sanctions reçoit les rapports et les procès-verbaux des contrôles.

(82) « *Art. L. 1332-16.* – La commission des sanctions mentionnée à l'article L. 1332-15 est composée :

(83) « 1° D'un membre du Conseil d'État, président, désigné par le vice-président du Conseil d'État, d'un membre de la Cour de cassation désigné par le premier président de la Cour de cassation, d'un membre de la Cour des comptes désigné par le premier président de la Cour des comptes ;

(84) « 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.

(85) « Un suppléant est désigné dans les mêmes conditions pour les membres mentionnés au 1° du présent article.

(86) « 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.

(87) « Le président de la commission désigne un rapporteur parmi ses membres. Celui-ci ne peut recevoir aucune instruction.

(88) « La procédure devant la commission des sanctions est contradictoire**.** Celle-ci 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.

(89) « La commission statue à la majorité des membres présents. En cas de partage égal des voix, celle du président est prépondérante.

(90) « Le président et les membres de la commission mentionnés au 1° ainsi que leurs suppléants respectifs sont nommés par décret.

(91) « Le mandat du président, des membres de la commission mentionnés au même 1° ainsi que de leurs suppléants respectifs est de cinq ans non renouvelable. Les membres sont tenus au secret professionnel.

(92) « *Art. L. 1332-17. – (Non modifié)* I. – En cas de manquement aux obligations découlant de l'application du présent chapitre, la commission des sanctions peut prononcer à l'encontre des opérateurs d'importance vitale, à

l'exception des administrations de l'État 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.

(93) « 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 maximal prévu au premier alinéa du présent I.

(94) « II. – En cas de manquement constaté aux obligations mentionnées à l'article 26 de la loi n° du 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 la même loi, peut prononcer les sanctions prévues aux articles 28 et 37 de ladite loi.

(95) « *Art. 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.

(96) « Le produit des sanctions pécuniaires est versé au Trésor public et recouvré comme les créances de l'État étrangères à l'impôt et au domaine.

(97) « Les recours formés contre les décisions de la commission des sanctions sont des recours de pleine juridiction.

(98) « *Art. L. 1332-19. – (Non modifié)* 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'État.

(99) *« Section 3*

(100) ***« Marchés publics et contrats de concession relatifs à la sécurité des activités d'importance vitale***

(101) « *Art. L. 1332-20. – (Non modifié)* Les marchés publics des opérateurs d'importance vitale mentionnés au I de l'article L. 1332-2 sont soumis aux règles définies au titre II du livre V de la deuxième partie du code de la commande publique lorsque :

(102) « 1° Ces marchés publics concernent la conception, la qualification, la fabrication, la modification, la maintenance ou le retrait des structures, des équipements, des systèmes, du matériel, des composants ou des logiciels qui sont nécessaires à la protection des infrastructures critiques de l'opérateur ou dont le détournement de l'usage porterait atteinte aux intérêts essentiels de l'État ;

(103) « 2° Et que cette protection ou la prévention de ce détournement d'usage ne peuvent être garanties par d'autres moyens.

(104) « *Art. L. 1332-21. – (Non modifié)* Les contrats de concession conclus par les opérateurs d'importance vitale mentionnés au I de l'article L. 1332-2 sont soumis aux règles définies au titre II du livre II de la troisième partie du code de la commande publique lorsque :

(105) « 1° Ces contrats de concession concernent la conception, la qualification, la fabrication, la modification, la maintenance ou le retrait des structures, des équipements, des systèmes, du matériel, des composants ou des logiciels qui sont nécessaires à la protection des infrastructures critiques de l'opérateur ou dont le détournement de l'usage porterait atteinte aux intérêts essentiels de l'État ;

(106) « 2° Et cette protection ou la prévention de ce détournement d'usage ne peuvent être garanties par d'autres moyens.

(107) « *Art. L. 1332-22. – (Non modifié)* Les opérateurs d'importance vitale qui passent un marché ou un contrat de concession en application des articles L. 1332-20 et L. 1332-21 en informent l'autorité administrative dans des conditions et des délais précisés par décret. »

CHAPITRE II

Dispositions diverses

Article 2

(1) I. – Le code de la défense est ainsi modifié :

(2) 1° Au dernier alinéa de l'article L. 1333-1, les mots : « certains établissements, installations ou ouvrages, relevant de l'article L. 1332-1 » sont remplacés par les mots : « certaines infrastructures des opérateurs d'importance vitale mentionnés au 1° du I de l'article L. 1332-2 » ;

③ 1° *bis (nouveau)* Au second alinéa de l'article L. 1411-2, les mots : « protection mentionnés à l'article L. 1332-3 » sont remplacés par les mots : « résilience mentionnés à l'article L. 1332-5 » ;

④ 2° À la fin du premier alinéa de l'article L. 2113-2, les mots : « établissements, aux installations ou aux ouvrages mentionnés aux articles L. 1332-1 et L. 1332-2 » sont remplacés par les mots : « opérateurs d'importance vitale mentionnés au I de l'article L. 1332-2 » ;

⑤ 3° Après le mot « personnel », la fin du deuxième alinéa de l'article L. 2151-1 est ainsi rédigée : « identifié dans les documents de planification des opérateurs désignés au titre de l'article L. 1332-2 visant à garantir la continuité de leur activité. » ;

⑥ 4° À l'article L. 2151-4, les mots : « d'élaborer des plans de continuité ou de rétablissement d'activité et de notifier aux personnes concernées par ces plans » sont remplacés par les mots : « de notifier aux personnes concernées » ;

⑦ 5° Au deuxième alinéa de l'article L. 2171-6, les mots : « publics et privés ou des gestionnaires d'établissements désignés par l'autorité administrative conformément aux articles L. 1332-1 et L. 1332-2 » sont remplacés par les mots : « d'importance vitale mentionnés au I de l'article L. 1332-2 » ;

⑧ 6° Aux premier et quatrième alinéas de l'article L. 2321-2-1, les mots : « mentionnés aux articles L. 1332-1 et L. 1332-2 » sont remplacés par les mots : « d'importance vitale mentionnés au I de l'article L. 1332-2 » ;

⑨ 7° L'article L. 2321-3 est ainsi modifié :

⑩ *a)* Au premier alinéa, les mots : « mentionnés aux articles L. 1332-1 et L. 1332-2 » sont remplacés par les mots : « d'importance vitale mentionnés au I de l'article L. 1332-2 » ;

⑪ *b)* À la première phrase du deuxième alinéa, les mots : « mentionné aux articles L. 1332-1 et L. 1332-2 » sont remplacés par les mots : « d'importance vitale mentionné au I de l'article L. 1332-2 » ;

⑫ 8° À l'article L. 4231-6, les mots : « publics ou privés ou par des gestionnaires d'établissements désignés par l'autorité administrative conformément aux articles L. 1332-1 et L. 1332-2 » sont remplacés par les mots : « d'importance vitale mentionnés au I de l'article L. 1332-2 ».

⑬ II. – *(Non modifié)* Au dernier alinéa de l'article 226-3 du code pénal, les mots : « mentionnés à l'article L. 1332-1 » sont remplacés par les mots : « d'importance vitale mentionnés au 1° du I de l'article L. 1332-2 ».

⑭ III. – *(Non modifié)* Le code des postes et des communications électroniques est ainsi modifié :

⑮ 1° Au *e* du I de l'article L. 33-1, les mots : « mentionnés aux articles L. 1332-1 et L. 1332-2 » sont remplacés par les mots : « d'importance vitale mentionnés au I de l'article L. 1332-2 » ;

⑯ 2° Au premier alinéa de l'article L. 33-14, les mots : « , mentionnés à l'article L. 1332-1 » sont remplacés par les mots : « d'importance vitale mentionnés au 1° du I de l'article L. 1332-2 » ;

⑰ 3° Au deuxième alinéa du I de l'article L. 34-11, les mots : « mentionnés à l'article L. 1332-1 » sont remplacés par les mots : « d'importance vitale mentionnés au 1° du I de l'article L. 1332-2 ».

⑱ IV. – *(Non modifié)* Aux 2° des II et VI de l'article L. 1333-9 du code de la santé publique, les mots : « certains établissements, installations ou ouvrages relevant de l'article L. 1332-1 » sont remplacés par les mots : « certaines infrastructures des opérateurs d'importance vitale mentionnés au 1° du I de l'article L. 1332-2 ».

⑲ V. – *(Non modifié)* Le code de la sécurité intérieure est ainsi modifié :

⑳ 1° Au 1° de l'article L. 223-2, les mots : « exploitants des établissements, installations ou ouvrages mentionnés aux articles L. 1332-1 et L. 1332-2 » sont remplacés par les mots : « opérateurs d'importance vitale mentionnés au I de l'article L. 1332-2 » ;

㉑ 2° À la première phrase du premier alinéa de l'article L. 223-8, les mots : « établissements, installations ou ouvrages mentionnés aux articles L. 1332-1 et L. 1332-2 » sont remplacés par les mots : « infrastructures des opérateurs d'importance vitale mentionnés au I de l'article L. 1332-2 ».

㉒ VI. – *(Non modifié)* Au troisième alinéa de l'article 15 de la loi n° 2006-961 du 1er août 2006 relative au droit d'auteur et aux droits voisins dans la société de l'information, les mots : « publics ou privés gérant des installations d'importance vitale au sens des articles L. 1332-1 à L. 1332-7 » sont remplacés par les mots : « d'importance vitale mentionnés au I de l'article L. 1332-2 ».

Article 3

① I. – *(Non modifié)* La sixième partie du code de la défense est ainsi modifiée :

② 1° Le chapitre Ier du titre II du livre II est complété par un article L. 6221-2 ainsi rédigé :

③ « *Art. L. 6221-2*. – En l'absence d'adaptation, les références faites, par des dispositions du présent code applicables à Saint-Barthélemy, à des dispositions qui n'y sont pas applicables sont remplacées par les références aux dispositions ayant le même objet applicables localement. » ;

④ 2° Au chapitre II du même titre II, il est ajouté un article L. 6222-1 ainsi rédigé :

⑤ « *Art. L. 6222-1*. – La sous-section 2 de la section 1 du chapitre II du titre III du livre III de la première partie n'est pas applicable à Saint-Barthélemy. » ;

⑥ 3° Le chapitre II du titre IV du livre II est complété par un article L. 6242-2 ainsi rédigé :

⑦ « *Art. L. 6242-2*. – La sous-section 2 de la section 1 du chapitre II du titre III du livre III de la première partie n'est pas applicable à Saint-Pierre-et-Miquelon. » ;

⑧ 4° Le chapitre II du titre Ier du livre III est complété par un article L. 6312-3 ainsi rédigé :

⑨ « *Art. L. 6312-3*. – La sous-section 2 de la section 1 du chapitre II du titre III du livre III de la première partie n'est pas applicable dans les îles Wallis et Futuna, en Polynésie française, en Nouvelle-Calédonie et dans les Terres australes et antarctiques françaises. »

⑩ II. – *(Non modifié)* L'article 711-1 du code pénal est ainsi rédigé :

⑪ « *Art. 711-1*. – Sous réserve des adaptations prévues au présent titre, les livres Ier à V du présent code sont applicables, dans leur rédaction résultant de la loi n° du relative à la résilience des infrastructures critiques et au renforcement de la cybersécurité, en Nouvelle-Calédonie, en Polynésie française et dans les îles Wallis et Futuna. »

⑫ III. – *(Non modifié)* Le chapitre II du titre Ier du livre II du code des postes et des communications électroniques est ainsi modifié :

⑬ 1° Après le mot « résultant », la fin du 1° du VII de l'article L. 33-1 est ainsi rédigée : « de la loi n° du relative à la résilience des infrastructures critiques et au renforcement de la cybersécurité. » ;

⑭ 2° Après le mot « résultant », la fin de l'article L. 33-15 est ainsi rédigée : « de la loi n° du relative à la résilience des infrastructures critiques et au renforcement de la cybersécurité. » ;

⑮ 3° L'article L. 34-14 est complété par les mots : « dans sa rédaction résultant de la loi n° du relative à la résilience des infrastructures critiques et au renforcement de la cybersécurité ».

⑯ IV. – Au premier alinéa des articles L. 285-1, L. 286-1, L. 287-1 et L. 288-1 du code de la sécurité intérieure, les mots : « n° 2025-532 du 13 juin 2025 visant à sortir la France du piège du narcotrafic » sont remplacés par les mots : « n° du relative à la résilience des infrastructures critiques et au renforcement de la cybersécurité ».

CHAPITRE III

Dispositions transitoires

Article 4

(Non modifié)

① Le présent titre entre en vigueur à une date fixée par décret en Conseil d'État, et au plus tard un an après la promulgation de la présente loi.

② Les opérateurs d'importance vitale désignés avant la date d'entrée en vigueur du présent titre sont regardés comme désignés en application du I de l'article L. 1332-2 du code de la défense dans sa rédaction résultant de la présente loi à la date de cette entrée en vigueur.

③ Ces opérateurs restent soumis aux obligations qui leur sont applicables avant l'entrée en vigueur du présent titre jusqu'à l'accomplissement des obligations prévues aux articles L. 1332-2 à L. 1332-5 et L. 1332-11 du code de la défense dans leur rédaction résultant de la présente loi.

TITRE II

CYBERSÉCURITÉ

CHAPITRE I^ER

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

Article 5

① L'autorité nationale de sécurité des systèmes d'information mentionnée à l'article L. 2321-1 du code de la défense 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.

② 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, en raison de leur activité dans le domaine de la défense, certaines des responsabilités de cette autorité prévues au présent titre.

③ Les missions de l'autorité nationale de sécurité des systèmes d'information et des organismes désignés par le Premier ministre ainsi que leurs conditions d'exercice sont précisées par décret en Conseil d'État. Ces missions comprennent notamment l'accompagnement et le soutien au développement de la filière cybersécurité en coordination avec les ministères compétents ainsi que la promotion de la cyberprotection de la cyberhygiène et de l'éducation aux bonnes pratiques numériques.

Article 5 *bis* A *(nouveau)*

À la seconde phrase du premier alinéa du I de l'article L. 731-3 du code de la sécurité intérieure, après le mot : « connus, », sont insérés les mots : « y compris le risque d'incident informatique ayant un impact important sur la fourniture des services à la population, ».

Article 5 *bis*

① Afin d'atteindre et de maintenir un niveau élevé de cybersécurité, le Premier ministre élabore une stratégie nationale qui comprend notamment :

② 1° Les objectifs et les priorités de la Nation en matière de cybersécurité et d'autonomie stratégique numérique, qui incluent en particulier les secteurs mentionnés à l'article 7 ;

③ 2° Une liste des différents organismes et autorités concernés par la mise en œuvre de cette stratégie nationale ;

④ 3° Une coordination renforcée entre les organismes et les autorités définis au 2° du présent article dans le but d'atteindre les objectifs et les priorités mentionnés au 1° ;

⑤ 4° Un inventaire des mesures garantissant le partage d'informations par les organismes et les autorités mentionnés au 2° sur les risques, les menaces et les incidents en matière de cybersécurité ainsi que la préparation, la réaction et la récupération des services après un incident ;

⑥ 4° *bis* Les orientations permettant une approche commune des enjeux de cybersécurité et de souveraineté numérique ;

⑦ 5° Un plan comprenant les mesures nécessaires pour améliorer le niveau général de sensibilisation des entreprises, des administrations publiques et des citoyens à la cybersécurité, notamment par des politiques actives de cyberprotection, de cyberhygiène et d'éducation aux bonnes pratiques numériques, annuellement mis en place dès 2026 et piloté par le dispositif national d'assistance aux victimes d'actes de cybermalveillance ;

⑧ 5° *bis* Les modalités de soutien, y compris financier, aux collectivités territoriales et à leurs groupements ;

⑨ 5° *ter* 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 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 ;

⑩ 5° *quater (nouveau)* L'offre de formation publique dans le domaine de la cybersécurité et la cyberdéfense ;

⑪ 5° *quinquies (nouveau)* Une stratégie d'aménagement du territoire en lien avec le 5° *ter* et comprenant :

⑫ *a)* Le maillage territorial des compétences, notamment par la création ou le soutien de centres régionaux de formation, d'expertise ou de réponse aux incidents ;

⑬ *b)* Les établissements d'enseignement supérieur, les lycées professionnels et les organismes de formation continue, en lien avec les régions ;

⑭ *c)* Les dispositifs de soutien aux collectivités territoriales pour leur mise en conformité, leur sécurisation numérique et leur capacité de résilience ;

⑮ *d)* Des objectifs de réduction des inégalités territoriales d'accès aux métiers, aux formations et aux ressources en cybersécurité ;

⑯ 5° *sexies (nouveau)* La création d'un fonds de soutien spécifiquement destiné à accompagner les collectivités territoriales et les établissements publics de coopération intercommunale à fiscalité propre qualifiés d'entités importantes ou essentielles n'ayant pas bénéficié du « parcours de **c**ybersécurité » du plan France relance ;

⑰ 5° *septies (nouveau)* Les orientations visant à promouvoir l'utilisation de logiciels libres et des standards ouverts comme leviers stratégiques pour la résilience, la sécurité et la souveraineté numérique de la Nation ;

⑱ 6° Les indicateurs clés de performance pour évaluer la mise en œuvre de la stratégie nationale en matière de cybersécurité.

⑲ La stratégie nationale en matière de cybersécurité est mise à jour au moins tous les trois ans.

⑳ À compter de 2026 puis tous les deux ans, le Gouvernement remet au Parlement, avant le 30 septembre, un rapport sur la mise en œuvre de la stratégie nationale en matière de cybersécurité. Ce rapport précise l'évolution des indices de performance définis par ladite stratégie.

CHAPITRE II

De la cyber-résilience

Section 1

Définitions

Article 6

① Au sens du présent titre, on entend par :

② 1° Bureau d'enregistrement : une entité fournissant des services d'enregistrement de noms de domaine ;

③ 1° *bis (nouveau)* Agent agissant pour le compte **d'un** bureau d'enregistrement : toute personne physique ou morale agissant pour le compte d'un bureau d'enregistrement, telle qu'un fournisseur de services d'anonymisation, un fournisseur de services d'enregistrement fiduciaire ou un revendeur de noms de domaine ;

④ 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. L'administration du domaine inclut l'enregistrement des noms de domaine en relevant et de son fonctionnement technique, notamment l'exploitation de ses serveurs de noms, la maintenance de ses bases de données et la distribution de ses fichiers de zone sur les serveurs de noms, que ces opérations soient effectuées par l'entité elle-même ou qu'elles soient sous-traitées, mais à l'exclusion des situations où les noms de domaine de premier niveau sont utilisés par un registre uniquement pour son propre usage ;

⑤ 2° *bis* 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 les systèmes d'information offrent ou rendent accessibles ;

⑥ 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 ;

⑦ 4° Prestataire de services de confiance qualifié : un prestataire de services de confiance au sens du paragraphe 20 du même article 3 ;

⑧ 5° Représentant : une personne physique ou morale établie dans l'Union européenne qui est expressément désignée pour agir pour le compte d'un fournisseur de services de système de nom de domaine, d'un office d'enregistrement, d'un bureau d'enregistrement, d'un agent agissant pour le compte d'un bureau d'enregistrement, 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 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 européenne, qui peut être contactée par une autorité compétente ou un centre de veille, d'alerte et de réponse aux attaques informatiques à la place de l'entité elle-même concernant les obligations incombant à ladite entité en application de la présente loi ;

⑨ 5° *bis (nouveau)* Résilience : la capacité d'un opérateur à prévenir tout type d'incident, à s'en protéger ou à y résister afin d'assurer la continuité de la ou des activités d'importance vitale qu'il exerce ;

⑩ 6° Service de centre de données : un service qui englobe les structures, ou les groupes de structures, consacrées à l'hébergement, à l'interconnexion et à 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 des infrastructures de distribution d'électricité et de contrôle environnemental ;

⑪ 7° Système d'information : l'ensemble des infrastructures et des services logiciels informatiques permettant de collecter, de traiter, de transmettre et de stocker des données sous forme numérique ;

⑫ 8° Vulnérabilité : une faiblesse, une susceptibilité ou une faille de produits ou de services des technologies de l'information et de la communication qui peut être exploitée par une cybermenace.

Section 2

Des exigences de sécurité des systèmes d'information

Article 7

① I. – Sont considérés, au titre de la présente section, comme des secteurs hautement critiques pour le fonctionnement de l'économie et de la société les secteurs :

② 1° De l'énergie ;

③ 2° Des transports ;

④ 3° Des banques ;

⑤ 4° Des infrastructures des marchés financiers ;

⑥ 5° De la santé ;

⑦ 6° De la distribution d'eau potable ;

⑧ 7° Des eaux usées ;

⑨ 8° De l'infrastructure numérique ;

⑩ 9° De la gestion des services des technologies de l'information et de la communication ;

⑪ 10° De l'espace.

⑫ II. – Sont considérés, au titre de la présente section, comme des secteurs critiques pour le fonctionnement de l'économie et de la société les secteurs :

⑬ 1° Des services postaux et d'expédition ;

⑭ 2° De la gestion des déchets ;

⑮ 3° De la fabrication, de la production et de la distribution de produits chimiques ;

⑯ 4° De la production, de la transformation et de la distribution des denrées alimentaires ;

⑰ 5° De la fabrication de certains biens, équipements et produits ;

⑱ 6° De la fourniture de certains services numériques ;

⑲ 7° De la recherche.

⑳ III. – *(Non modifié)* Un décret en Conseil d'État précise les modalités d'application du présent article. Il détermine les sous-secteurs et les types d'entités relevant des secteurs mentionnés aux I et II.

Article 8

① Sont des entités essentielles :

② 1° Les entreprises, à l'exception de celles dont tout ou partie des activités sont soumises à autorisation au titre de l'article L. 1333-2 du code de la défense pour ces seules activités, relevant d'un type d'entités 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 ;

③ 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 mentionnées au 2° de l'article L. 2221-4 du code général des collectivités territoriales, à l'exception des établissements publics ou des régies précités dont tout ou partie des activités sont soumises à autorisation au titre de l'article L. 1333-2 du code de la défense pour ces seules activités, relevant d'un type d'entités appartenant à un des secteurs d'activité hautement critiques, qui emploient au moins 250 personnes ou dont les produits d'exploitation excèdent 50 millions d'euros et le total du bilan annuel excède 43 millions d'euros. Le critère d'emploi est calculé selon les modalités prévues au I de l'article L. 130-1 du code de la sécurité sociale, les critères financiers sont appréciés au niveau de la personne morale ou de la régie concernée ;

④ 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 ;

⑤ 4° Les prestataires de services de confiance qualifiés ;

⑥ 5° Les offices d'enregistrement ;

⑦ 6° Les fournisseurs de services de système de noms de domaine et les éditeurs de logiciels ;

⑧ 7° Les administrations suivantes :

⑨ *a)* Les administrations de l'État et leurs établissements publics administratifs, à l'exception des administrations de l'État qui exercent leurs activités dans les domaines de la sécurité publique, de la défense et de la sécurité nationale, de la répression pénale et des missions diplomatiques et consulaires françaises pour leurs réseaux et leurs 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'État qui, compte tenu du faible impact économique et social de leur activité, ne sont pas soumis à la présente loi, dans des conditions précisées par décret en Conseil d'État ;

⑩ *b)* Les régions, les départements, les communes d'une population supérieure à 30 000 habitants, ainsi que leurs établissements publics administratifs dont les activités s'inscrivent dans un des secteurs d'activité hautement critiques ou critiques ;

⑪ *c)* Les centres de gestion de la fonction publique territoriale mentionnés à l'article L. 452-1 du code général de la fonction publique ;

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

⑬ *e)* Les communautés urbaines, les communautés d'agglomération et les métropoles ainsi que leurs établissements publics administratifs dont les activités s'inscrivent dans un des secteurs d'activité hautement critiques ou critiques ;

⑭ *f)* Les syndicats mentionnés aux articles L. 5212-1, L. 5711-1 et L. 5721-2 du même code dont les activités s'inscrivent dans un des secteurs d'activité hautement critiques ou critiques et dont la population est supérieure à 30 000 habitants ;

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

⑯ *g) bis (nouveau)* Les établissements publics de santé au sens de l'article L. 6141-1 du code de la santé publique ;

⑰ *g) ter (nouveau)* Les établissements et services sociaux et médico-sociaux au sens de l'article L. 312-1 du code de l'action sociale et des familles ;

⑱ *h)* Et les autres organismes et personnes de droit public ou de droit privé à compétence nationale 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 l'exception de ceux qui sont désignés entité importante par arrêté du Premier ministre. Le Premier ministre désigne par arrêté les organismes et les personnes morales qui, compte tenu du faible impact économique et social de leur activité, ne sont pas soumis à la présente loi, dans des conditions précisées par décret en Conseil d'État ;

⑲ 8° Les opérateurs d'importance vitale, à l'exception des opérateurs d'importance vitale dont tout ou partie des activités sont soumises à autorisation au titre de l'article L. 1333-2 du code de la défense pour ces seules activités, en tant qu'ils exercent une activité qualifiée de service essentiel en application du second alinéa du 1° du I de l'article L. 1332-2 du même code ;

⑳ 9° Les opérateurs offrant des services essentiels désignés en application de l'article 5 de la loi n° 2018-133 du 26 février 2018 portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité avant l'entrée en vigueur de la présente loi, à l'exception de ces opérateurs dont tout ou partie des activités sont soumises à autorisation au titre de l'article L. 1333-2 du code de la défense pour ces seules activités ;

㉑ 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'État, qui remplissent l'un des critères mentionnés à l'article 10 de la présente loi.

Article 9

① Sont des entités importantes, lorsqu'**ils** ne sont pas des entités essentielles :

② 1° Les entreprises, à l'exception de celles dont tout ou partie des activités sont soumises à autorisation au titre de l'article L. 1333-2 du code de la défense pour ces seules activités, relevant d'un type d'entités appartenant à un des secteurs d'activité hautement critiques ou critiques 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 ;

③ 2° Les opérateurs de communications électroniques ;

④ 3° Les prestataires de services de confiance ;

⑤ 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 ;

⑥ 5° Les établissements d'enseignement menant des activités de recherche. 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 des conditions précisées par décret en Conseil d'État ;

⑦ 6° Les établissements publics administratifs de l'État expressément désignés en tant qu'entités importantes par arrêté du Premier ministre dans des conditions fixées par décret en Conseil d'État ;

⑧ 6° *bis (nouveau)* Les établissements publics de santé au sens de l'article L. 6141-1 du code de la santé publique ;

⑨ 6° *ter (nouveau)* Les établissements et services sociaux et médico-sociaux au sens de l'article L. 312-1 du code de l'action sociale et des familles ;

⑩ 7° Les autres organismes et personnes de droit public ou de droit privé à compétence nationale 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, expressément désignés en tant qu'entités importantes par arrêté du Premier ministre dans des conditions précisées par décret en Conseil d'État ;

⑪ 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 mentionnées au 2° de l'article L. 2221-4 du code général des collectivités territoriales, à l'exception de ces opérateurs dont tout ou partie des activités sont soumises à autorisation au titre de l'article L. 1333-2 du code de la défense pour ces seules activités, relevant d'un type d'entités appartenant à un 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. Le critère d'emploi est calculé selon les modalités prévues au I de l'article L. 130-1 du code de la sécurité sociale, les

critères financiers sont appréciés au niveau de la personne morale ou de la régie concernée.

Article 10

① I. – Outre les entités mentionnées aux articles 8 et 9, le Premier ministre, après avis des ministres compétents **pour les** secteurs d'activité **mentionnés** à l'article 7, 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 1° L'entité est, sur le territoire national, le seul prestataire d'un service qui est essentiel au maintien du fonctionnement de la société et d'activités économiques critiques ;

③ 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 ;

④ 3° Une perturbation du service fourni par l'entité pourrait induire un risque systémique important, en particulier dans les secteurs où cette perturbation pourrait avoir un impact transfrontière ;

⑤ 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.

⑥ II. *(nouveau)* – Le Premier ministre peut, par arrêté, exempter certaines personnes mentionnées à l'article 14 qui exercent des activités dans les domaines de la sécurité nationale, de la sécurité publique, de la défense ou de la répression pénale ou qui fournissent des services exclusivement aux administrations de l'État et **à** leurs établissements publics à caractère administratif exerçant ces activités de certaines obligations prévues aux articles 14 et 17, en ce qui concerne ces activités ou services.

Article 11

(Non modifié)

① I. – Les entités essentielles et les entités importantes sont régies par le présent titre lorsque, selon le cas :

② 1° Elles sont établies sur le territoire national ;

③ 2° S'agissant des opérateurs de communications électroniques, ils fournissent leurs services sur le territoire national ;

④ 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 :

⑤ *a)* Ils ont leur établissement principal sur le territoire national ;

⑥ *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.

⑦ Toutefois, les conditions d'établissement sur le territoire national ne s'appliquent pas aux administrations et aux établissements publics.

⑧ II. – Les obligations prévues au présent titre applicables aux bureaux d'enregistrement et aux agents agissant pour le compte de ces derniers concernent :

⑨ 1° Ceux qui ont leur établissement principal sur le territoire national ;

⑩ 2° Ou ceux qui ont désigné un représentant établi sur le territoire national, s'ils sont établis hors de l'Union européenne mais offrent leurs services sur le territoire national.

⑪ III. – Pour l'application des I et II, l'établissement principal s'entend du lieu où sont principalement prises les décisions relatives aux mesures de gestion des risques en matière de cybersécurité ou, à défaut, du lieu où les opérations de cybersécurité sont effectuées ou, à défaut, de l'établissement comptant le plus grand nombre de salariés dans l'Union européenne.

Article 12

① L'autorité nationale de sécurité des systèmes d'information établit et met à jour au moins tous les deux ans la liste des entités essentielles, des entités importantes, des bureaux d'enregistrement et des agents agissant pour le compte de ces derniers sur la base des informations que ces entités,

ces bureaux d'enregistrement et **les** agents agissant pour le compte de ces derniers lui communiquent, après avis des ministres compétents **pour les** secteurs d'activité mentionnés à l'article 7.

② Dans le respect des modalités de chiffrement de bout en bout ainsi que de protection des données recueillies de l'effet des lois extraterritoriales, les informations à transmettre, leurs modalités de communication et les délais dans lesquels les modifications doivent être transmises sont définis par un décret en Conseil d'État pris après avis de la **C**ommission nationale de l'informatique et des libertés **prévue** par la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

Article 13

Les dispositions des articles 14, 15 et 17, y compris celles relatives à la supervision s'agissant du respect des mêmes articles 14, 15 et 17, 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. Pour être équivalentes, les exigences de notification des incidents doivent également prévoir un accès immédiat aux notifications d'incident par l'autorité nationale de sécurité des systèmes d'information.

Article 14

① Les entités essentielles, les entités importantes, les administrations de l'État et leurs établissements publics administratifs qui exercent leurs activités dans les domaines de la sécurité publique, de la défense et de la sécurité nationale ainsi que de la répression pénale, les missions diplomatiques et consulaires françaises pour leurs réseaux et systèmes d'information, le Commissariat à l'énergie atomique et aux énergies alternatives pour ses activités dans le domaine de la défense, les personnes morales qui exercent des activités soumises à autorisation au titre de l'article L. 1333-2 du code de la défense et qui, de ce fait, sont exclues en tout partie de la qualification d'entité essentielle ou importante, pour ces seules activités, ainsi que les juridictions administratives et judiciaires mettent en œuvre, à leurs frais, les mesures techniques, opérationnelles et organisationnelles appropriées et proportionnées pour gérer les risques qui menacent les réseaux et les systèmes d'information qu'ils 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 usagers de

leurs services et sur d'autres services. Ces mesures garantissent, pour leurs réseaux et leurs systèmes d'information, un niveau de sécurité et de résilience adapté et proportionné au risque existant. Le choix de ces mesures tient compte de leur capacité à être audités, de la transparence de leur fonctionnement, de leur interopérabilité, de leur résilience et de la maîtrise qu'elles permettent d'acquérir sur les systèmes d'information afin de minimiser les dépendances technologiques à l'égard de prestataires tiers ne présentant pas de garanties suffisantes de conformité aux exigences de cybersécurité et de souveraineté numérique fixées par la stratégie nationale dans une perspective de long terme. Elles visent à :

② 1° Prévoir que les organes de direction approuvent et supervisent les mesures de pilotage de la sécurité des réseaux et des systèmes d'information. Les membres de ces organes ainsi que les personnes exposées aux risques doivent être formés à la cybersécurité en fonction de leur degré d'exposition au risque ;

③ 2° Assurer la protection des réseaux et systèmes d'information, y compris en cas de recours à la sous-traitance ;

④ 3° Mettre en place des outils et des procédures pour assurer la défense des réseaux et des systèmes d'information et gérer les incidents ;

⑤ 4° Garantir la résilience des activités, des réseaux et des systèmes d'information.

⑥ Un décret en Conseil d'État fixe les objectifs auxquels doivent se conformer les personnes mentionnées au premier alinéa du présent article 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, en fonction de leur degré d'exposition aux risques, de leur taille, de la probabilité de survenance d'incidents et de la gravité de ceux-ci, y compris leurs conséquences économiques et sociales.

⑦ Ce décret fixe les modalités de concertation avec les ministères, **l**es représentants des entités concernées et **les** associations d'élus pour le référentiel mentionné au huitième alinéa.

⑧ Ce référentiel peut prescrire le recours à des produits, des services ou des processus certifiés au titre du règlement (UE) n° 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (Agence de

l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) n° 526/2013 (règlement sur la cybersécurité).

⑨ Par dérogation aux sixième et septième alinéas du présent article, lorsqu'ils sont des entités importantes ou essentielles, 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 définies par le **r**èglement d'exécution (UE) 2024/2690 de la Commission du 17 octobre 2024 établissant des règles relatives à l'application de la directive (UE) 2022/2555 pour ce qui est des exigences techniques et méthodologiques liées aux mesures de gestion des risques en matière de cybersécurité et précisant plus en détail les cas dans lesquels un incident est considéré comme important, en ce qui concerne les fournisseurs de services DNS, les registres des noms de domaine de premier niveau, les fournisseurs de services d'informatique en nuage, les fournisseurs de services de centres de données, les fournisseurs de réseaux de diffusion de contenu, les fournisseurs de services gérés, les fournisseurs de services de sécurité gérés, ainsi que les fournisseurs de places de marché en ligne, de moteurs de recherche en ligne et de plateformes de services de réseaux sociaux, et les prestataires de services de confiance pris en application 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 , en veillant au respect des principes énoncés au premier alinéa du présent article.

⑩ Les personnes mentionnées au **même** premier alinéa peuvent se prévaloir auprès de l'**a**utorité nationale de sécurité des systèmes d'information, lors d'un contrôle, du recours à des prestataires de services qualifiés pour démontrer leur respect de tout ou partie des objectifs mentionnés au sixième alinéa, dans des conditions fixées par décret en Conseil d'État.

Article 15

① Les personnes mentionnées au premier alinéa de l'article 14 qui mettent en œuvre les exigences du référentiel mentionné au huitième alinéa du même

article 14 ou qui mettent en œuvre tout autre référentiel reconnu comme équivalent par l'autorité nationale de sécurité des systèmes d'information peuvent s'en prévaloir auprès de l'autorité nationale de sécurité des systèmes d'information lors d'un contrôle pour démontrer le respect des objectifs mentionnés au septième alinéa dudit article 14.

② Lorsque ces personnes bénéficient d'un label de confiance approuvé par l'autorité nationale de sécurité des systèmes d'information, elles sont présumées conformes jusqu'à preuve du contraire, à ces mêmes objectifs. Ce label est sans préjudice de l'exercice des missions et des pouvoirs de contrôle prévus au chapitre III des agents et des personnels mentionnés à l'article 26.

③ Un décret en Conseil d'État précise :

④ 1° Les conditions de reconnaissance de l'équivalence des normes et des spécifications techniques européennes ou internationales pour la sécurité des réseaux et des systèmes permettant aux personnes mentionnées au premier alinéa de l'article 14 de démontrer leur conformité à tout ou partie des objectifs mentionnés au septième alinéa du même article 14 ;

⑤ 2° Les conditions de reconnaissance de l'équivalence de normes en matière de sécurité des réseaux et des systèmes d'information adoptées par des États membres en application de l'article 21 de la directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures permettant aux entités essentielles ou importantes qui fournissent des services dans ces États membres et auraient, dans ces derniers, la qualification d'entité importante ou essentielle, de démontrer leur conformité à tout ou partie des objectifs mentionnés au septième alinéa de l'article 14 de la présente loi.

⑥ Ce décret fixe les modalités de concertation avec les ministères, les représentants des entités concernées et les associations d'élus pour les conditions mentionnées au 2° du présent article.

⑦ Dans le cas contraire, ces personnes sont tenues de démontrer que les mesures qu'elles mettent en œuvre permettent de se conformer à ces objectifs.

Article 16

① Les opérateurs mentionnés à l'article L. 1332-2 du code de la défense recensent, tiennent à jour et communiquent à l'autorité nationale de sécurité des systèmes d'information la liste de leurs systèmes d'information

d'importance vitale mentionnés au *b* du 2° de l'article L. 1332-1 du même code selon des modalités déterminées par le Premier ministre.

② Ces opérateurs mettent en œuvre sur leurs systèmes d'information d'importance vitale les exigences du référentiel mentionné à l'article 14 de la présente loi ainsi que les exigences spécifiques à ces systèmes d'information définies par le Premier ministre.

③ Les administrations qui sont des entités essentielles ou importantes ainsi que les administrations de l'État et leurs établissements publics administratifs qui exercent leurs activités dans les domaines de la sécurité publique, de la défense et de la sécurité nationale ou de la répression pénale, les missions diplomatiques et consulaires françaises pour leurs réseaux et systèmes d'information ainsi que les juridictions administratives et judiciaires mettent en œuvre les exigences du référentiel mentionné au même article 14 ainsi que les exigences spécifiques définies par le Premier ministre à l'égard des systèmes d'information permettant des échanges d'informations par voie électronique avec le public et d'autres administrations.

④ Les exigences spécifiques mentionnées aux trois premiers alinéas du présent article peuvent prescrire le recours à des dispositifs matériels ou logiciels ou à des prestataires de services certifiés, qualifiés ou agréés ou prévoir que ce recours à des dispositifs matériels ou logiciels ou à des prestataires de services certifiés, qualifiés ou agréés emporte présomption de conformité à l'exigence de sécurité concernée. Ces exigences peuvent également prévoir la réalisation régulière d'audits de sécurité réguliers par des organismes indépendants. Les personnes mentionnées au présent article appliquent ces exigences à leurs frais.

Article 16 *bis*

Il ne peut être imposé aux fournisseurs de services de chiffrement, y compris aux prestataires de services de confiance qualifiés, l'intégration de dispositifs techniques visant à affaiblir volontairement la sécurité des systèmes d'information et des communications électroniques tels que des clés de déchiffrement maîtresses ou tout autre mécanisme ou processus permettant un accès non consenti aux données protégées.

Article 17

① I. – 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.

② Un incident est considéré comme important s'il :

③ 1° A causé ou est susceptible de causer une perturbation opérationnelle grave des services ou des pertes financières significatives pour la personne concernée ;

④ 2° A affecté ou est susceptible d'affecter d'autres personnes physiques ou morales en causant des dommages matériels, corporels ou moraux considérables.

⑤ II. – Les personnes mentionnées à l' article 14 soumettent à l'autorité nationale de sécurité des systèmes d'information :

⑥ *a)* Sans retard injustifié et au plus tard vingt-quatre heures après avoir eu connaissance de l'incident important, une notification initiale qui, le cas échéant, indique si l'incident important est susceptible d'avoir été causé par des actes illicites ou malveillants ou s'il pourrait avoir un impact en dehors du territoire national ;

⑦ *b)* Sans retard injustifié et au plus tard soixante-douze heures après avoir eu connaissance de l'incident important, une notification intermédiaire qui met à jour les informations mentionnées au *a* du présent II 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. Par dérogation, les entités mentionnées au 4° de l'article 8 et au 3° de l'article 9 procèdent à cette notification sans retard injustifié et au plus tard vingt-quatre heures après avoir eu connaissance de l'incident important ayant un impact sur la fourniture de leurs services de confiance ;

⑧ *c)* À la demande de l'autorité nationale de sécurité des systèmes d'information, un rapport sur les mises à jour pertinentes de la situation ;

⑨ *d)* Au plus tard un mois après la notification intermédiaire mentionnée au *b* du présent II, un rapport final, sous réserve que l'incident soit traité ;

⑩ *e)* Dans le cas contraire, un rapport d'avancement, au plus tard un mois après la notification intermédiaire mentionnée au même *b*, devant être

complété par un rapport final dans un délai d'un mois à compter du traitement de l'incident.

⑪ L'autorité nationale de sécurité des systèmes d'information fournit, sans retard injustifié et si possible dans les vingt-quatre heures suivant la réception de la première notification reçue, une réponse à la personne émettrice de la notification.

⑫ Pour prévenir un incident concernant une entité essentielle ou une entité importante ou pour faire face à un incident en cours ou lorsque la divulgation de l'incident est dans l'intérêt public, 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.

⑬ III. – Le cas échéant, les entités essentielles et importantes notifient sans retard injustifié aux destinataires de leurs services :

⑭ 1° Les incidents importants ayant un impact direct sur les destinataires de leurs services, notamment lorsqu'ils ont causé ou sont susceptibles de causer l'extraction de données sensibles de ces derniers ou de causer la mort ou des dommages considérables à la santé d'une personne physique destinataire ou lorsqu'ils consistent en un accès non autorisé effectif au réseau et aux systèmes d'information de l'entité, susceptible d'être malveillant et de causer une perturbation opérationnelle grave pour le destinataire ;

⑮ 2° Toutes les mesures ou corrections que ces destinataires peuvent appliquer en réponse à une vulnérabilité critique qui les affecterait potentiellement. Le cas échéant, les entités informent également ces destinataires de la vulnérabilité critique elle-même.

⑯ L'obligation de notification prévue au présent III ne s'étend pas aux informations dont la divulgation porterait atteinte aux intérêts de la défense et de la sécurité nationale.

⑰ IV. – En cas d'incident important ou de vulnérabilité critique, les personnes mentionnées au premier alinéa du I peuvent communiquer à l'autorité nationale de sécurité des systèmes d'information la liste des destinataires de leurs services. Cette autorité tient compte, dans l'usage qu'elle fait de ces informations, des intérêts économiques de ces personnes et veille à ne pas révéler d'informations susceptibles de porter atteinte à leur sécurité et au secret en matière commerciale et industrielle.

⑱ V. – L'autorité nationale de sécurité des systèmes d'information informe la Commission nationale de l'informatique et des libertés de tout incident mentionné au premier alinéa du I susceptible d'entraîner une violation de données à caractère personnel.

⑲ VI. – Un décret en Conseil d'État détermine les modalités d'application du présent article. Il précise notamment la procédure applicable et les critères d'appréciation du caractère important et critique des incidents et des vulnérabilités.

Section 3

Enregistrement des noms de domaine

Article 18

Les offices d'enregistrement et les bureaux d'enregistrement ainsi que les agents agissant pour le compte de ces derniers qui remplissent l'une des conditions prévues à l'article 11 sont soumis à la présente section.

Article 19

① Les offices d'enregistrement collectent, par l'intermédiaire des bureaux d'enregistrement et des agents agissant pour le compte de ces derniers, les données nécessaires à l'enregistrement des noms de domaine, y compris les données du point de contact qui gère le nom de domaine, si ces coordonnées sont différentes de celles du titulaire, notamment en cas de recours à des services permettant l'anonymisation des données d'enregistrement.

② Les offices et les bureaux d'enregistrement ainsi que les agents agissant pour le compte de ces derniers 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. À cette fin, ils mettent en place des procédures, accessibles au public, permettant de vérifier ces données et d'assurer la sécurité de leur base de données.

③ Un décret en Conseil d'État, pris après avis de la Commission nationale de l'informatique et des libertés, dresse la liste des données relatives aux noms de domaine devant être collectées et précise les procédures de vérification des données d'enregistrement des noms de domaine.

Article 20

Les offices et les bureaux d'enregistrement ainsi que les agents agissant pour le compte de ces derniers conservent les données relatives à chaque nom de domaine dans leur base de données pendant la durée d'utilisation du nom de domaine et jusqu'à l'expiration d'un délai d'un an à compter de la cessation de l'utilisation de ce nom de domaine.

Article 21

Les offices et les bureaux d'enregistrement ainsi que les agents agissant pour le compte de ces derniers rendent publiques, sans retard injustifié après l'enregistrement d'un nom de domaine, les données d'enregistrement relatives à ce nom de domaine si elles n'ont pas de caractère personnel.

Article 22

① Pour les besoins des procédures pénales et de la sécurité des systèmes d'information, les agents habilités à cet effet par l'autorité judiciaire ou par l'autorité nationale de sécurité des systèmes d'information peuvent obtenir, de la part des offices et des bureaux d'enregistrement ainsi que des agents agissant pour le compte de ces derniers, les données mentionnées à l'article 20.

② Afin de permettre la détection de faits et de circonstances caractérisant une violation de droits consacrés par le code de la propriété intellectuelle susceptible d'une qualification pénale, les agents mentionnés à l'article L. 331-2 du même code et les auxiliaires de justice qualifiés par la loi pour dresser des procès-verbaux constatant ces faits et circonstances peuvent obtenir des offices et bureaux d'enregistrement, sur production des constats effectués, les données mentionnées à l'article 20 de la présente loi.

③ Les offices et les bureaux d'enregistrement ainsi que les agents agissant pour le compte de ces derniers définissent les règles de procédure pour la communication de ces données aux agents mentionnés aux deux premiers alinéas du présent article. Cette communication intervient dans un délai de soixante-douze heures. Ces règles sont accessibles au public.

④ Un décret en Conseil d'État, pris après avis de la Commission nationale de l'informatique et des libertés, définit les modalités d'application du présent article.

Section 4

Coopération et échange d'informations

Article 23

① L'article 11 du code de procédure pénale ou les dispositions 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, les autorités compétentes chargées de la gestion des risques en matière de cybersécurité en application d'un acte sectoriel de l'Union européenne, les autorités chargées de la conduite de la politique pénale, de l'action publique et de l'instruction, la Commission européenne, les autorités compétentes des autres États membres de l'Union européenne, 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.

② La communication d'informations effectuée en application du premier alinéa du présent article ne peut intervenir que si elle est nécessaire à l'accomplissement des missions des personnes émettrices ou destinataires de ces informations. Les informations échangées se limitent au nécessaire et sont proportionnées à l'objectif du partage. Le partage d'informations préserve la confidentialité des informations concernées et protège la sécurité des entités concernées.

③ Les modalités d'application du présent article, notamment les modalités du partage d'informations, sont déterminées par décret en Conseil d'État.

Article 24

① 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 agréés sont autorisés à échanger entre eux des informations couvertes par des secrets protégés par la loi.

② 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'État.

CHAPITRE III

De la supervision

Article 25

① Lorsqu'elle a connaissance d'une menace susceptible de porter atteinte à la sécurité des systèmes d'information des personnes mentionnées à l'article 14, des bureaux d'enregistrement et des agents agissant pour le compte de ces derniers, l'autorité nationale de sécurité des systèmes d'information peut prescrire à la personne, au bureau d'enregistrement concerné ou aux agents agissant pour le compte de ce dernier les mesures nécessaires pour éviter un incident ou y remédier et déterminer les délais accordés pour les mettre en œuvre et en rendre compte.

② Les modalités d'application du présent article sont fixées par décret en Conseil d'État.

Section 1

Recherche et constatations des manquements

Sous-section 1

Habilitation

Article 26 A

① L'article L. 103 du code des postes et des communications électroniques est ainsi modifié :

② 1° L'avant-dernier alinéa est supprimé ;

③ 2° *(nouveau)* Au dernier alinéa, les mots : « et de sa certification par l'État » sont supprimés.

Article 26

① Les agents et personnels spécialement désignés et assermentés de l'autorité nationale de sécurité des systèmes d'information et des services de l'État désignés par elle sont habilités à rechercher et à constater les manquements aux obligations, aux prescriptions et aux exigences prévues :

② 1° Par 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 n° 1999/93/CE ;

③ 2° Par le règlement (UE) n° 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) n° 526/2013 (règlement sur la cybersécurité) ;

④ 3° Au chapitre II du présent titre et au présent chapitre ;

⑤ 4° À l'article L. 100 et aux III et IV de l'article L. 102 du code des postes et des communications électroniques ;

⑥ 4° *bis (nouveau)* À l'article L. 1332-11 du code de la défense ;

⑦ 5° Par les exigences de cybersécurité résultant des autorisations, des certifications, des qualifications et des agréments délivrés par l'autorité nationale de sécurité des systèmes d'information ou, le cas échéant, par les organismes d'évaluation de la conformité ;

⑧ 6° *(nouveau)* Aux articles 39, 41, 47 et 49 du règlement (UE) 2024/2847 du Parlement européen et du Conseil du 23 octobre 2024 concernant des exigences de cybersécurité horizontales pour les produits comportant des éléments numériques et modifiant les règlements (UE) n° 168/2013 et (UE) 2019/1020 et la directive (UE) 2020/1828 (règlement sur la cyberrésilience).

⑨ Les agents et personnels des organismes indépendants ou les experts spécialement habilités par l'autorité nationale de sécurité des systèmes d'information peuvent concourir à la recherche des manquements mentionnés au premier alinéa du présent article sous le contrôle des agents et personnels mentionnés au même premier alinéa.

Sous-section 2

Des pouvoirs

Article 27

① La personne faisant l'objet d'un contrôle de l'autorité nationale de sécurité des systèmes d'information met à la disposition des agents et personnels mentionnés à l'article 26 les moyens nécessaires pour vérifier sur pièces et sur place le respect des obligations mentionnées au même article 26.

② Ces agents et personnels ont accès aux locaux à usage professionnel des entités contrôlées et sont habilités à :

③ 1° Exiger la communication de tout document nécessaire à l'accomplissement de leur mission, quel qu'en soit le support, et obtenir ou prendre copie de ces documents par tout moyen et sur tout support ;

④ 2° Recueillir, sur convocation, sur place ou sur demande, tout renseignement ou toute justification nécessaire au contrôle ;

⑤ 3° Accéder, lorsque cela est directement nécessaire à l'accomplissement de leur mission, aux systèmes d'information, aux logiciels, aux programmes informatiques et aux données stockées et en demander la transcription par tout traitement approprié dans des documents directement exploitables pour les besoins de la supervision ;

⑥ 4° Procéder, sur convocation ou sur place, aux auditions de toute personne susceptible d'apporter des éléments utiles à leurs constatations. Ils en dressent un procès-verbal. Les personnes entendues procèdent elles-mêmes à sa lecture, peuvent y faire consigner leurs observations et y apposent leur signature. Si elles déclarent ne pas pouvoir lire, lecture leur en est faite préalablement à la signature. En cas de refus de signer le procès-verbal, mention en est faite sur celui-ci ;

⑦ 5° *(nouveau)* Prélever des échantillons de produits, dans des conditions fixées par décret en Conseil d'État, pour l'application des 1°, 2°, 4° et 5° de l'article 26. Les rapports d'essais ou d'analyses des échantillons prélevés peuvent être transmis aux personnes concernées. Dans le cadre de la recherche et de la constatation des manquements, les échantillons dont la non-conformité aux obligations et aux réglementations mentionnées aux

mêmes 1°, 2°, 4° et 5° n'a pas été établie sont restitués ou remboursés à leur valeur au jour du prélèvement toutes taxes comprises.

⑧ Dans le cadre du contrôle, le secret professionnel ne peut être opposé aux agents et personnels mentionnés au premier alinéa du présent article.

⑨ Ces agents et personnels sont tenus au secret professionnel pour les faits, les actes ou les renseignements dont ils ont connaissance en raison de leurs fonctions, sous réserve des éléments utiles à l'établissement des documents nécessaires à l'instruction.

⑩ Les rapports, les avis et les autres documents justifiant la saisine de la commission des sanctions mentionnée à l'article L. 1332-15 du code de la défense en application de l'article 28 de la présente loi ou l'adoption d'une mesure d'exécution prévue à l'article 31, y compris ceux établis ou recueillis dans le cadre des opérations de contrôle, peuvent être communiqués à la personne contrôlée.

⑪ Il est dressé un procès-verbal des vérifications et des visites menées en application du présent article, qui fait foi jusqu'à preuve du contraire.

Article 28

① La personne faisant l'objet d'un contrôle de l'autorité nationale de sécurité des systèmes d'information est tenue de coopérer avec les agents et personnels mentionnés à l'article 26, qui sont habilités à constater toute action de sa part de nature à faire obstacle au contrôle.

② Le fait, pour la personne contrôlée, de faire obstacle aux contrôles, notamment en fournissant des renseignements incomplets ou inexacts ou en communiquant des pièces incomplètes ou dénaturées, est constitutif d'un manquement et puni d'une amende administrative prononcée par la commission des sanctions mentionnée à l'article L. 1332-15 du code de la défense, dont le montant, proportionné à la gravité du manquement, ne peut excéder :

③ 1° Pour les entités essentielles, dix millions d'euros ou 2 % du chiffre d'affaires annuel mondial, hors taxes, de l'exercice précédent, le montant le plus élevé étant retenu ;

④ 2° *(nouveau)* Pour les entités importantes, sept millions d'euros ou 1,4 % du chiffre d'affaires annuel mondial total, hors taxes, de l'exercice précédent, le montant le plus élevé étant retenu.

⑤ L’autorité nationale de sécurité des systèmes d’information notifie à la personne contrôlée les griefs constitutifs d’un obstacle, au sens du deuxième alinéa du présent article, retenus à son encontre et saisit la commission des sanctions mentionnée à l’article L. 1332-15 du code de la défense, qui se prononce dans les conditions prévues à la section 3 du présent chapitre.

⑥ Le présent article ne s’applique ni aux administrations de l’État ni à ses établissements publics administratifs.

Article 29

① Le contrôle de l’autorité nationale de sécurité des systèmes d’information peut prendre les formes suivantes :

② 1° Des inspections sur place et des contrôles à distance ;

③ 2° Des audits de sécurité réguliers et ciblés réalisés par l’autorité nationale de sécurité des systèmes d’information ;

④ 2° *bis* Des audits de sécurité réguliers et ciblés réalisés par un organisme indépendant désigné par l’autorité nationale de sécurité des systèmes d’information ;

⑤ 3° Des scans de sécurité ;

⑥ 4° Des audits en cas d’incident important ou d’une violation des obligations mentionnées à l’article 26.

⑦ Le coût des mesures mentionnées aux 1°, 2°, 3° et 4° du présent article est à la charge de l’autorité nationale de sécurité des systèmes d’information. Celui des mesures mentionnées au 2° *bis* est à la charge de la personne contrôlée sauf, lorsque les circonstances l’exigent, si l’autorité nationale de sécurité des systèmes d’information en décide autrement.

⑧ Lorsque les exigences spécifiques mentionnées aux trois premiers alinéas de l'article 16 prescrivent le recours à des prestataires de services certifiés, qualifiés ou agréés ou à des audits de sécurité réguliers réalisés par des organismes indépendants, l’autorité nationale de sécurité des systèmes d’information est tenue de proposer aux entités mentionnées à l’article 14 une liste comprenant, le cas échéant, plusieurs prestataires de services certifiés, qualifiés ou agréés ou organismes indépendants parmi lesquels celles-ci doivent choisir. Les entités mentionnées au même article 14 notifient, le cas échéant, à l’autorité nationale de sécurité des systèmes

d'information le prestataire de services certifiés, qualifiés ou agréés ou l'organisme indépendant qu'elles ont choisi.

Article 30

(Non modifié)

Les modalités d'application de la présente section sont fixées par décret en Conseil d'État.

Section 2

Mesures consécutives aux contrôles

Article 31

① Au vu des résultats du contrôle réalisé en application de la section 1 du présent chapitre, l'autorité nationale de sécurité des systèmes d'information peut ouvrir une procédure. Le cas échéant, elle en informe la personne contrôlée.

② L'instruction est confiée à un ou plusieurs rapporteurs désignés parmi les agents et personnels mentionnés à l'article 26.

③ Lorsque les faits constatés ne justifient pas l'adoption d'une mesure d'exécution mentionnée aux 1° à 5° du présent article, l'autorité nationale de sécurité des systèmes d'information clôt la procédure et en informe la personne contrôlée.

④ Dans le cas contraire, l'autorité nationale de sécurité des systèmes d'information peut, après avoir mis la personne contrôlée en mesure de présenter ses observations :

⑤ 1° Prononcer un avertissement à son encontre ;

⑥ 2° Lui enjoindre de prendre les mesures nécessaires pour éviter un incident ou y remédier et d'en rendre compte dans un délai qu'elle détermine ;

⑦ 3° Lui enjoindre de se mettre en conformité avec les obligations mentionnées à l'article 26 dans un délai qu'elle détermine et qui ne peut être inférieur à un mois, sauf en cas de manquement grave ou répété ;

⑧ 4° Lui enjoindre d'informer les personnes physiques ou morales auxquelles elle fournit des services ou au profit desquelles elle exerce des activités susceptibles d'être affectés par une menace de nature à porter gravement atteinte à la sécurité des systèmes d'information de la nature de cette menace et de suggérer à ces personnes des mesures préventives ou réparatrices ;

⑨ 5° Lui enjoindre de mettre en œuvre, dans un délai qu'elle détermine, les recommandations formulées à la suite d'un audit de sécurité.

⑩ La mesure d'exécution adoptée est notifiée à la personne contrôlée et peut être assortie d'une astreinte prononcée par l'autorité nationale de sécurité des systèmes d'information, dont le montant ne peut excéder 5 000 euros par jour de retard.

⑪ L'astreinte journalière court à compter du lendemain de l'expiration du délai imparti à la personne contrôlée pour se mettre en conformité avec la mesure d'exécution notifiée. En cas d'inexécution totale ou partielle ou d'exécution tardive, la commission des sanctions mentionnée à l'article L. 1332-15 du code de la défense procède à la liquidation de l'astreinte.

Article 32

(Suppression maintenue)

Article 33

① Lorsque la personne contrôlée fournit des éléments montrant qu'elle s'est mise en conformité avec la mesure d'exécution notifiée en application de l'article 31 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 en informe la personne contrôlée.

② Dans le cas contraire, l'autorité nationale de sécurité des systèmes d'information notifie à la personne contrôlée les griefs retenus à son encontre et saisit la commission des sanctions mentionnée à l'article L. 1332-15 du code de la défense.

③ Lorsque la personne contrôlée est une entité essentielle ou une personne morale qui exerce des activités soumises à autorisation au titre de l'article L. 1333-2 du même code et qui, de ce fait, est exclue, en tout ou partie, de la qualification d'entité essentielle, pour ces seules activités, et

qu'elle n'apporte pas la preuve qu'elle s'est mise en conformité avec les mesures d'exécution mentionnées aux 2°, 3° et 5° de l'article 31 de la présente loi 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 la personne contrôlée jusqu'à ce que celle-ci ait mis un terme au manquement. Lorsque cette certification ou cette autorisation a été délivrée par un organisme de certification ou d'autorisation, l'autorité nationale de sécurité des systèmes d'information enjoint à cet organisme de la suspendre jusqu'à ce que la personne contrôlée ait mis un terme au manquement.

Article 33 *bis (nouveau)*

① Les actes mentionnés au présent titre établis par les agents et personnels mentionnés à l'article 26 peuvent être établis ou convertis sous format numérique et peuvent être intégralement conservés sous cette forme, dans des conditions sécurisées, sans nécessité d'un support papier.

② Lorsque ces actes sont établis sous format numérique et que les dispositions du présent titre exigent qu'ils soient signés, ils font l'objet, quel qu'en soit le nombre de pages et pour chaque signataire, d'une signature unique sous forme numérique, selon des modalités techniques qui garantissent que l'acte ne peut plus ensuite être modifié. Ces actes n'ont pas à être revêtus d'un sceau.

③ Les modalités d'application du présent article sont précisées par voie réglementaire.

Article 34

Un décret en Conseil d'État définit les modalités de la procédure prévue à la présente section.

Section 3

Des sanctions

Article 35

(Non modifié)

Saisie par l'autorité nationale de sécurité des systèmes d'information, 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 du chapitre II du présent titre et du présent chapitre, dans les conditions prévues à la présente section.

Article 36

① Lorsqu'elle est saisie par l'autorité nationale de sécurité des systèmes d'information de manquements aux obligations découlant de l'application du chapitre II du présent titre et du présent chapitre, la commission des sanctions mentionnée à l'article L. 1332-15 du code de la défense est composée :

② 1° Des personnes mentionnées au 1° de l'article L. 1332-16 du même code ;

③ 2° De trois personnalités qualifiées, nommées respectivement par le Premier ministre, le Président de l'Assemblée nationale et le Président du Sénat en raison de leurs compétences dans le domaine de la sécurité des systèmes d'information.

Article 37

① I. – En cas de manquement aux obligations prévues au présent titre, la commission des sanctions peut prononcer :

② 1° À l'encontre des entités essentielles, des personnes morales qui exercent des activités soumises à autorisation au titre de l'article 1333-2 du code de la défense et qui, de ce fait, sont exclues en tout ou partie de la qualification d'entité essentielle, pour ces seules activités, et des opérateurs mentionnés à l'article L. 1332-2 du même code, à l'exception des administrations de l'État 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 2 % du chiffre d'affaires annuel mondial, hors taxes, de l'exercice précédent de l'entreprise à laquelle la personne concernée appartient, le montant le plus élevé étant retenu ;

③ 2° À l'encontre des entités importantes et des personnes morales qui exercent des activités soumises à autorisation au titre de l'article L. 1333-2 du code de la défense et qui, de ce fait sont exclues en tout ou partie de la qualification d'entité importante, pour ces seules activités, à l'exception des administrations de l'État 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 sept millions d'euros ou 1,4 % du chiffre d'affaires annuel mondial total, hors taxes, de l'exercice précédent de l'entreprise à laquelle la personne concernée appartient, le montant le plus élevé étant retenu ;

④ 3° À l'encontre des offices d'enregistrement, des bureaux d'enregistrement et des agents agissant pour le compte de ces derniers 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 sept 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° du présent I prononcée à l'encontre d'un office d'enregistrement en cas de manquement aux obligations applicables aux entités essentielles.

⑤ Si les manquements relevés constituent également une violation du règlement (UE) n° 2016/679 du Parlement européen et du Conseil 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 (règlement général sur la protection des données) donnant lieu à une amende administrative prononcée par la Commission nationale de l'informatique et des libertés en application 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.

⑥ II. – La commission des sanctions peut prononcer une amende administrative dont le montant, proportionné à la gravité du manquement, ne

peut excéder dix 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 :

⑦ 1° Des fournisseurs de moyens d'identification électronique relevant des schémas d'identification électronique notifiés par l'État, des prestataires de services de confiance établis sur le territoire français, des fournisseurs de dispositifs de création de signature et de cachet électronique qualifié que l'autorité nationale de sécurité des systèmes d'information certifie et des organismes d'évaluation de la conformité, à l'exception des administrations de l'État et de leurs établissements publics à caractère administratif, en cas de manquement constaté au règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 précité ;

⑧ 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 et de cybersécurité, des titulaires d'un agrément, d'une qualification ou d'un certificat dans le domaine de la cybersécurité, en cas de manquement constaté aux exigences mentionnées aux 2°, 4°, 5° et 6° de l'article 26 de la présente loi.

⑨ III. – *(Non modifié)* Lorsque la commission des sanctions envisage de prononcer l'amende prévue à l'article 28 à l'encontre de la même personne, le montant cumulé des sanctions ne peut excéder le montant maximum de l'amende prévue aux I ou II du présent article.

⑩ IV. – *(Non modifié)*La commission des sanctions peut également prononcer 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 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, du 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 (règlement sur la cybersécurité) ou des exigences de cybersécurité mentionnées au 5° de l'article 26 de la présente loi, les mesures suivantes :

⑪ 1° L'abrogation d'un agrément, d'une qualification ou d'un certificat ;

⑫ 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.

⑬ V. – La commission des sanctions peut, si les mesures d'exécution prévues aux articles 25 et 31 sont inefficaces, 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. Le présent V ne s'applique pas aux administrations.

⑭ VI. – *(Non modifié)* Lorsque la commission des sanctions prononce l'une des sanctions prévues aux I à IV, elle peut exiger que l'entité concernée communique au public, par tout moyen adapté et à ses frais, le manquement constaté.

⑮ La commission des sanctions peut décider, dans l'intérêt du public, de rendre publique sa décision ou un extrait de celle-ci, selon des modalités qu'elle précise.

⑯ VII. – *(Non modifié)* Lorsque la commission des sanctions prononce l'une des sanctions prévues au présent article, elle prend en compte les circonstances et la gravité du manquement, le comportement de son auteur, notamment sa bonne foi, ainsi que ses ressources et ses charges.

Article 37 *bis (nouveau)*

Les organismes d'évaluation de la conformité peuvent évaluer la conformité à des exigences de cybersécurité et délivrer les certificats de conformité lorsque les schémas de certification le prévoient, le cas échéant, après autorisation de l'autorité nationale de sécurité des systèmes d'information.

CHAPITRE IV

Dispositions diverses d'adaptation

Article 38

① Le titre III de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique est ainsi modifié :

② 1° L'article 30 est ainsi modifié :

③ *a)* Au II, les mots : « la communauté » sont remplacés par les mots : « l'Union » ;

④ *b)* Le III est ainsi rédigé :

⑤ III. – « La fourniture, le transfert depuis ou vers un État membre de l'Union européenne, l'importation et l'exportation d'un moyen de cryptologie n'assurant pas exclusivement des fonctions d'authentification ou de contrôle d'intégrité sont soumis à une déclaration préalable au Premier ministre, à l'exception, sans préjudice des exigences applicables aux biens à double usage intégrant un moyen de cryptologie, des moyens dont les caractéristiques techniques ou les conditions d'utilisation sont telles, au regard des intérêts de la défense nationale et de la sécurité intérieure ou extérieure de l'État, qu'ils peuvent être dispensés de toute formalité préalable. Un décret en Conseil d'État fixe les conditions dans lesquelles sont souscrites ces déclarations, les conditions et les délais dans lesquels le Premier ministre peut demander communication des caractéristiques du moyen ainsi que la nature de ces caractéristiques. » ;

⑥ *c)* Le IV est abrogé ;

⑦ 2° L'article 33 est abrogé ;

⑧ 3° Le I de l'article 35 est ainsi rédigé :

⑨ « I. – Sans préjudice de l'application du code des douanes, le fait de ne pas satisfaire à l'obligation de déclaration prévue à l'article 30 en cas de fourniture, de transfert depuis ou vers un État membre de l'Union européenne, d'importation ou d'exportation d'un moyen de cryptologie est puni d'un an d'emprisonnement et de 15 000 euros d'amende. »

Article 39

① I. – Le chapitre I^{er} du titre II du livre III de la deuxième partie du code de la défense est ainsi modifié :

② 1° L'article L. 2321-2-1 est ainsi modifié :

③ *a)* Au premier alinéa, la première occurrence du mot : « ou » est remplacée par le signe : « , » et les mots : « à 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 » sont remplacés par les

mots : « des entités essentielles au sens des articles 8 et 10 de la loi n° du relative à la résilience des infrastructures critiques et au renforcement de la cybersécurité » ;

④ *b)* Au quatrième alinéa, les mots : « à l'article 5 de la loi n° 2018-133 du 26 février 2018 précitée » sont remplacés par les mots : « des entités essentielles au sens des articles 8 et 10 de la loi n° du précitée » ;

⑤ 2° L'article L. 2321-3 est ainsi modifié :

⑥ *a)* Au premier alinéa, les mots : « opérateurs mentionnés à 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 » sont remplacés par les mots : « entités essentielles au sens des articles 8 et 10 de la loi n° du relative à la résilience des infrastructures critiques et au renforcement de la cybersécurité » ;

⑦ *b)* Au deuxième alinéa, les mots : « ou à l'article 5 de la loi n° 2018-133 du 26 février 2018 précitée » sont remplacés par les mots : « , d'une entité essentielle au sens des articles 8 et 10 de la loi n° du précitée ».

⑧ II. – Le code des postes et des communications électroniques est ainsi modifié :

⑨ 1° L'article L. 33-1 est ainsi modifié :

⑩ *a)* À la fin du *a* du I, les mots : « qui incluent des obligations de notification à l'autorité compétente des incidents de sécurité ayant eu un impact significatif sur leur fonctionnement » sont supprimés ;

⑪ *b)* Après le *q* du même I, il est inséré un *r* ainsi rédigé :

⑫ « *r)* Les prescriptions en matière de sécurité des systèmes d'information prévues par la loi n° du relative à la résilience des infrastructures critiques et au renforcement de la cybersécurité. » ;

⑬ *c)* À l'avant-dernier alinéa dudit I, les mots : « et *o* » sont remplacés par les mots : « , *o* et *r* » ;

⑭ *d)* Le VII est complété par un 4° ainsi rédigé :

⑮ « 4° Le *r* du I est applicable en Polynésie française, dans les îles Wallis et Futuna et en Nouvelle-Calédonie dans sa rédaction résultant de la loi n° du relative à la résilience des infrastructures critiques et au renforcement de la cybersécurité. » ;

⑯ 2° Après le deuxième alinéa de l'article L. 45, il est inséré un alinéa ainsi rédigé :

⑰ « Chaque office d'enregistrement est responsable du fonctionnement technique du domaine de premier niveau qui lui est attribué, dont l'exploitation de ses serveurs de noms de domaine, la maintenance de ses bases de données d'enregistrement et la distribution des fichiers de zone du domaine de premier niveau sur les serveurs de noms de domaine, qu'il effectue lui-même ces opérations ou qu'elles soient sous-traitées. » ;

⑱ 3° Au deuxième alinéa de l'article L. 45-3, après le mot : « territoire », sont insérés les mots : « de l'un des États membres » ;

⑲ 4° L'article 45-4 est ainsi modifié :

⑳ *a)* La première phrase du premier alinéa est complétée par les mots : « ainsi que par les agents agissant pour le compte de ces derniers définis au 2° *ter* de l'article 6 de la loi n° du relative à la résilience des infrastructures critiques et au renforcement de la cybersécurité » ;

㉑ *b)* À la seconde phrase du même premier alinéa, après le mot : « enregistrement », sont insérés les mots : « ni aux agents agissant pour le compte de ces derniers » ;

㉒ *c)* Le dernier alinéa est complété par une phrase ainsi rédigée : « Les bureaux d'enregistrement sont responsables vis-à-vis de l'office d'enregistrement du respect de ces règles par les agents agissant pour leur compte. » ;

㉓ *d) (Supprimé)*

㉔ 5° L'article L. 45-5 est ainsi modifié :

㉕ *a)* Le deuxième alinéa est ainsi rédigé :

㉖ « Les offices d'enregistrement, par l'intermédiaire des bureaux d'enregistrement ainsi que des agents agissant pour le compte de ces derniers, collectent les données nécessaires à l'enregistrement des noms de domaine, notamment celles relatives à l'identification des personnes physiques ou morales titulaires de ces noms de domaine et des personnes chargées de leur gestion. Après l'enregistrement, et sans retard injustifié, les offices et les bureaux d'enregistrement rendent publiques, au moins quotidiennement, ces données si elles n'ont pas de caractère personnel. Ils tiennent ces bases de données à jour, en maintenant les données exactes et

complètes, sans redondance de collecte, et sont responsables du traitement de ces données dans le respect de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. » ;

㉗ *b)* À la première phrase du dernier alinéa, après le mot : « inexactes », sont insérés les mots : « ou incomplètes » ;

㉘ *c)* Sont ajoutés trois alinéas ainsi rédigés :

㉙ « Pour les besoins des procédures pénales et de la sécurité des systèmes d'information, les agents habilités à cet effet par l'autorité judiciaire ou par l'autorité nationale de sécurité des systèmes d'information peuvent obtenir les données d'enregistrement mentionnées au deuxième alinéa.des offices et bureaux d'enregistrement, ainsi que des agents agissant pour le compte de ces derniers.

㉚ « Les offices d'enregistrement, les bureaux d'enregistrement et les agents agissant pour le compte de ces derniers répondent aux demandes d'accès aux données d'enregistrement dans un délai de soixante-douze heures à compter de la réception de la demande.

㉛ « Le décret en Conseil d'État prévu à l'article L. 45-7 fixe la liste des données d'enregistrement devant être collectées. » ;

㉜ 6° L'article L. 45-8 est complété par les mots : « dans leur rédaction résultant de la loi n° du relative à la résilience des infrastructures critiques et au renforcement de la cybersécurité ».

㉝ III. – *(Non modifié)* Le titre I^{er} 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 est abrogé.

㉞ IV. – *(Non modifié)*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 est ainsi modifiée :

㉟ 1° Les 2° et 3° du II de l'article 1er sont abrogés ;

㊱ 2° Les articles 9 et 12 sont abrogés ;

㊲ 3° Le I de l'article 14 est abrogé.

㊳ V *(nouveau)*. – Au IV de l'article 42 de la loi n° 2018-727 du 10 août 2018 pour un État au service d'une société de confiance, les mots : « des articles 9 à 12 » sont remplacés par les mots :

« de l'article 11 » et après la dernière occurrence du mot : « administratives », sont insérés les mots : « ainsi qu'à celles relatives aux exigences spécifiques à l'égard des systèmes d'information permettant des échanges d'informations par voie électronique avec le public et d'autres administrations mentionnées au troisième alinéa de l'article 16 de la loi n° du relative à la résilience des infrastructures critiques et au renforcement de la cybersécurité ».

㊴ VI *(nouveau)*. – Au dernier alinéa de l'article 29-4 de la loi n° 90-568 du 2 juillet 1990 relative à l'organisation du service public de la poste et à France Télécom, les mots : « des articles 9 à 12 » sont remplacés par les mots : « de l'article 11 » et, après la dernière occurrence du mot : « administratives », sont insérés les mots : « ainsi qu'à celles relatives aux exigences spécifiques à l'égard des systèmes d'information permettant des échanges d'informations par voie électronique avec le public et d'autres administrations mentionnées au troisième alinéa de l'article 16 de la loi n° du relative à la résilience des infrastructures critiques et au renforcement de la cybersécurité ».

㊵ VII *(nouveau)*. – À la seconde phrase de l'article L. 212-3 du code des relations entre le public et l'administration, les mots : « règles du référentiel général de sécurité mentionné au I de l'article 9 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 remplacés par les mots : « exigences spécifiques à l'égard des systèmes d'information permettant des échanges d'informations par voie électronique avec le public et d'autres administrations mentionnées au troisième alinéa de l'article 16 de la loi n° du relative à la résilience des infrastructures critiques et au renforcement de la cybersécurité ».

Article 40

① I. – Le présent titre, à l'exception de l'article 13 et des 2° à 6° du II de l'article 39, est applicable en Polynésie française et en Nouvelle-Calédonie, sous réserve des adaptations suivantes :

② 1° Sous réserve du présent article, les références faites par des dispositions du présent titre 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 ;

③ 2° Les sanctions pécuniaires encourues en application du présent titre sont prononcées en monnaie locale, compte tenu de la contre-valeur de l'euro dans cette monnaie.

④ I *bis*. – *(Non modifié)* Le présent titre, à l'exception de l'article 13, est applicable dans les îles Wallis et Futuna et dans les Terres australes et antarctiques françaises. Toutefois, dans les îles Wallis et Futuna les sanctions pécuniaires encourues en application du présent titre sont prononcées en monnaie locale, compte tenu de la contre-valeur de l'euro dans cette monnaie.

⑤ II. – *(Non modifié)* L'article 13 n'est pas applicable à Saint-Barthélemy et à Saint-Pierre-et-Miquelon.

⑥ III. – Pour l'application du présent titre à Saint-Barthélemy, à 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 modifiant le règlement (UE) n° 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148, au règlement (UE) n° 2016/679 du Parlement européen et du Conseil du 27 avril 2016 précité, au règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 précité et au règlement (UE) n° 2019/881 du Parlement européen et du Conseil du 17 avril 2019 précité sont remplacées par la référence aux règles en vigueur en métropole en application des mêmes règlements.

⑦ IV. – *(Non modifié)* Le I de l'article 57 de la loi n° 2004-575 du 21 juin 2004 précitée est ainsi modifié :

⑧ 1° Au premier alinéa, les mots : « et 29 » sont remplacés par les mots : « , 29 à 31 et 37 » et, à la fin, les mots : « n° 2024-449 du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique » sont remplacés par les mots : « n° du relative à la résilience des infrastructures critiques et au renforcement de la cybersécurité » ;

⑨ 2° Au deuxième alinéa, les mots : « et 29 » sont remplacés par les mots : « , 29 à 31 et 37 » et sont ajoutés les mots : « dans leur rédaction résultant de la loi n° du relative à la résilience des infrastructures critiques et au renforcement de la cybersécurité » ;

⑩ 3° Au dernier alinéa, les mots : « 35 à » sont remplacés par la référence : « 37, » et la référence : « 34 » est remplacée par les références : « 31, 37 ».

⑪ V. – *(Non modifié)* Le I de l'article 24 de la loi n° 2018-133 du 26 février 2018 portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité est ainsi rédigé :

⑫ « I. – Le titre V est applicable à Wallis-et-Futuna, en Polynésie française, en Nouvelle-Calédonie et dans les Terres australes et antarctiques françaises, dans sa rédaction résultant de la présente loi. »

⑬ VI. – *(Non modifié)* L'article 16 de l'ordonnance n° 2005-1516 du 8 décembre 2005 précitée est complété par les mots : « dans sa rédaction résultant de la loi n° du relative à la résilience des infrastructures critiques et au renforcement de la cybersécurité ».

CHAPITRE V

Dispositions relatives aux communications électroniques

Article 41

① L'article L. 39-1 du code des postes et des communications électroniques est ainsi modifié :

② 1° Au début du premier alinéa, est ajoutée la mention : « I. – » ;

③ 2° Les 2° à 4° sont remplacés par un 2° ainsi rédigé :

④ « 2° D'utiliser une fréquence, un équipement ou une installation radioélectrique :

⑤ « *a)* Dans des conditions non conformes à l'article L. 34-9 ;

⑥ « *b)* Sans posséder l'autorisation prévue à l'article L. 41-1 ;

⑦ « *c)* Sans respecter les conditions de cette autorisation lorsque celle-ci est requise ;

⑧ « *d)* Sans posséder le certificat d'opérateur prévu à l'article L. 42-4 ;

⑨ « *e)* Sans respecter les conditions réglementaires générales prévues à l'article L. 33-3 ;

⑩ « *f)* Sans l'accord ou l'avis mentionné au I de l'article L. 43 ou sans respecter les caractéristiques déclarées lors de la demande de cet accord ou de cet avis. » ;

⑪ 3° Sont ajoutés des II et III ainsi rédigés :

⑫ « II. – Est puni de trois ans d'emprisonnement et de 75 000 euros d'amende, sous réserve de l'application de l'article 78 de la loi n° 86-1067 du 30 septembre 1986 relative à la liberté de communication, le fait :

⑬ « 1° De perturber les émissions hertziennes d'un service autorisé en utilisant une fréquence, un équipement ou une installation radioélectrique :

⑭ « *a)* Dans des conditions non conformes à l'article L. 34-9 du présent code ;

⑮ « *b)* Sans posséder l'autorisation prévue à l'article L. 41-1 ;

⑯ « *c)* Sans respecter les conditions de cette autorisation lorsque celle-ci est requise ;

⑰ « *d)* Sans posséder le certificat d'opérateur prévu à l'article L. 42-4 ;

⑱ « *e)* En dehors des conditions réglementaires générales prévues à l'article L. 33-3 ;

⑲ « *f)* Sans l'accord ou l'avis mentionné au I de l'article L. 43 ou sans respecter les caractéristiques déclarées lors de la demande de cet accord ou de cet avis ;

⑳ « 2° De perturber les émissions hertziennes d'un service autorisé en utilisant un appareil, un équipement ou une installation, électrique ou électronique, dans des conditions non conformes à la réglementation régissant la compatibilité électromagnétique des équipements électriques et électroniques.

㉑ « III. – Est puni de cinq ans d'emprisonnement et de 150 000 euros d'amende le fait :

㉒ « 1° D'avoir pratiqué l'une des activités prohibées par le I de l'article L. 33-3-1 en dehors des cas prévus au II du même article L. 33-3-1 ;

㉓ « 2° D'utiliser, sans l'autorisation prévue au premier alinéa de l'article L. 41-1, des fréquences attribuées par le Premier ministre en application de l'article L. 41 pour les besoins de la défense nationale et de la sécurité

publique ou d'utiliser une installation radioélectrique, en vue d'assurer la réception de signaux transmis sur ces mêmes fréquences, sans l'autorisation prévue au deuxième alinéa de l'article L. 41-1. »

Article 42

① I. – L'article L. 97-2 du code des postes et communications électroniques est ainsi modifié :

② 1° Le I est ainsi modifié :

③ *a)* Le second alinéa du 1 est remplacé par cinq alinéas ainsi rédigés :

④ « L'Agence nationale des fréquences déclare, au nom de la France, l'assignation de fréquence correspondante à l'Union internationale des télécommunications et engage la procédure prévue par le règlement des radiocommunications.

⑤ « Cette déclaration est effectuée sous réserve :

⑥ « *a)* De la conformité de l'assignation demandée au tableau national de répartition des bandes de fréquences et aux stipulations des instruments de l'Union internationale des télécommunications ;

⑦ « *b)* De l'existence d'un intérêt économique ou d'un intérêt pour la défense nationale justifiant que la déclaration soit effectuée au nom de la France ;

⑧ « *c)* Que l'assignation soumise ne soit pas de nature à compromettre les intérêts de la sécurité nationale et le respect par la France de ses engagements internationaux. » ;

⑨ *b)* Le 2 est ainsi modifié :

⑩ – après le deuxième alinéa, il est inséré un alinéa ainsi rédigé :

⑪ « L'autorisation est octroyée à une entité de droit français ou à un établissement immatriculé au registre du commerce et des sociétés en France. » ;

⑫ – au 1°, après le mot : « défense », il est inséré le mot : « nationale » et sont ajoutés les mots : « ainsi que le respect par la France de ses engagements internationaux » ;

⑬ – après le 4°, sont insérés des 5° et 6° ainsi rédigés :

⑭ « 5° Lorsque le demandeur ne peut démontrer que l'autorisation présente un intérêt économique pour la France ;

⑮ « 6° Lorsque le demandeur serait dans l'incapacité technique ou financière de faire face durablement à ses obligations une fois l'autorisation obtenue. » ;

⑯ *c)* Il est ajouté un alinéa ainsi rédigé :

⑰ « Elle 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. » ;

⑱ 2° Le second alinéa du III est remplacé par onze alinéas ainsi rédigés :

⑲ « Lorsque le titulaire de l'autorisation ne se conforme pas, dans le délai imparti, à la mise en demeure qui lui a été adressée, le ministre chargé des communications électroniques peut lui notifier des griefs.

⑳ « Après que l'intéressé a reçu la notification des griefs et a été mis à même de consulter le dossier et de présenter ses observations écrites, le ministre chargé des communications électroniques procède, avant de prononcer une sanction, à son audition selon une procédure contradictoire.

㉑ « Le ministre chargé des communications électroniques peut, en outre, entendre toute personne dont l'audition lui paraît utile.

㉒ « Le ministre chargé des communications électroniques peut prononcer à l'encontre du titulaire de l'autorisation l'une des sanctions suivantes :

㉓ « 1° La suspension totale ou partielle, pour un mois au plus, de l'autorisation, la réduction de sa durée, dans la limite d'une année, ou son retrait ;

㉔ « 2° Une sanction pécuniaire dont le montant est proportionné à la gravité du manquement et aux avantages qui en sont retirés, sans pouvoir excéder 3 % du chiffre d'affaires hors taxes du dernier exercice clos, ou 5 % de celui-ci en cas de nouvelle violation de la même obligation. À défaut d'activité permettant de déterminer ce plafond, le montant de la sanction ne peut excéder 150 000 euros, ou 375 000 euros en cas de nouvelle violation de la même obligation ;

㉕ « 3° L'interruption de la procédure engagée par la France auprès de l'Union internationale des télécommunications.

㉖ « Lorsque le manquement est constitutif d'une infraction pénale, le montant total des sanctions pécuniaires prononcées ne peut excéder le montant de la sanction encourue le plus élevé.

㉗ « Lorsque le ministre chargé des communications électroniques a prononcé une sanction pécuniaire devenue définitive avant que le juge pénal ait statué sur les mêmes faits ou des faits connexes, ce dernier peut ordonner que la sanction pécuniaire s'impute sur l'amende qu'il prononce.

㉘ « Les sanctions pécuniaires sont recouvrées comme les créances de l'État étrangères à l'impôt et au domaine.

㉙ « Les décisions du ministre chargé des communications électroniques sont motivées et notifiées à l'intéressé. Elles peuvent être rendues publiques dans les publications, les journaux ou les services de communication au public par voie électronique choisis par le ministre, dans un format et pour une durée proportionnés à la sanction infligée. Elles peuvent faire l'objet d'un recours de pleine juridiction. » ;

㉚ 3° Les 1° à 4° du VI sont remplacés par des 1° à 7° ainsi rédigés :

㉛ « 1° Les conditions dans lesquelles l'Agence nationale des fréquences déclare, au nom de la France, les assignations de fréquence à l'Union internationale des télécommunications ;

㉜ « 2° La procédure selon laquelle les autorisations sont délivrées ou retirées et selon laquelle leur caducité est constatée ;

㉝ « 3° Les conditions dont les autorisations d'exploitation peuvent être assorties ;

㉞ « 4° La durée et les conditions de modification et de renouvellement de l'autorisation ;

㉟ « 5° Les conditions de mise en service du système satellitaire ;

㊱ « 6° Les modalités d'établissement et de recouvrement de la redevance prévue au deuxième alinéa du 2 du I ;

㊲ « 7° Les modalités des procédures de mise en demeure et de sanction prévues au III. »

㊳ II. – *(Non modifié)* À l'article L. 97-4 du code des postes et des communications électroniques, après la référence : « L. 97-2 », sont insérés les mots : « , dans sa rédaction résultant de la loi n° du relative à la résilience des infrastructures critiques et au renforcement de la cybersécurité, ».

㊴ III. – Le présent article s'applique à compter de l'entrée en vigueur du décret prévu au VI de l'article L. 97-2 du code des postes et des communications électroniques, et au plus tard du 31 décembre 2025.

TITRE III

RÉSILIENCE OPÉRATIONNELLE NUMÉRIQUE DU SECTEUR FINANCIER

CHAPITRE IER

Dispositions modifiant le code monétaire et financier

Article 43 A

① Le code monétaire et financier est ainsi modifié :

② 1° *(Supprimé)*

③ 2 Après l'article L. 612-24, il est inséré un article L. 612-24-1 ainsi rédigé :

④ « *Art. L. 612-24-1.* – I. – En application du premier alinéa du paragraphe 1 de l'article 19 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 entités financières soumises à ce règlement qui relèvent de la compétence de l'Autorité de contrôle prudentiel et de résolution, à l'exception des personnes mentionnées au *b* du 2° du A du I de l'article L. 612-2 du présent code, adressent à l'Autorité de contrôle prudentiel et de résolution leurs déclarations d'incidents majeurs liés aux technologies de l'information et de la communication.

⑤ « Lorsque ces entités sont également soumises, en tant qu'entités essentielles ou importantes, aux dispositions de la directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des

mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union modifiant, elles transmettent également à l'autorité nationale de sécurité des systèmes d'information, en application du sixième alinéa du paragraphe 1 de l'article 19 du règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 précité, leurs déclarations d'incidents majeurs liés aux technologies de l'information et de la communication.

⑥ « II. – *(nouveau)* En application du paragraphe 2 de l'article 19 du règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 précité, les entités financières mentionnées au premier alinéa du I du présent article peuvent adresser à l'Autorité de contrôle prudentiel et de résolution leurs notifications de cybermenaces. Dans ce cas, elles transmettent également ces notifications à l'autorité nationale de sécurité des systèmes d'information. »

⑦ 3° *(nouveau)* Après la vingt-deuxième ligne du tableau du second alinéa du I des articles L. 783-2, L. 784-2 et L. 785-2, est insérée une ligne ainsi rédigée :

⑧

« L. 612-24-1	la loi n° du	»

Article 43

(Non modifié)

Au 7° du III de l'article L. 314-1 du code monétaire et financier, après les mots : « de l'information », sont insérés les mots : « et de la communication ».

Article 44

① L'article L. 420-3 du code monétaire et financier est ainsi modifié :

② 1° Le I est ainsi modifié :

③ *a)* À la première phrase, les mots : « des systèmes, des procédures et des mécanismes efficaces assurant » sont remplacés par les mots : « et maintient sa résilience opérationnelle conformément aux exigences prévues 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 pour garantir » et le mot : « tension » est remplacé par les mots : « graves tensions » ;

④ *b)* À la deuxième phrase, après le mot : « tests », il est inséré le mot : « exhaustifs » et, à la fin, les mots : « dans des situations d'extrême volatilité des marchés » sont supprimés ;

⑤ *c)* À la dernière phrase, après le mot : « activités », sont insérés les mots : « , y compris une politique et des plans en matière de continuité des activités liées aux technologies de l'information et de la communication et des plans de réponse et de rétablissement des technologies de l'information et de la communication élaborés en application de l'article 11 du règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 précitée afin d'assurer le maintien de ses services, » ;

⑥ 2° Le III est ainsi modifié :

⑦ *a)* Au premier alinéa, après la seconde occurrence du mot : « tests », sont insérés les mots : « conformément aux exigences fixées aux chapitres II et IV du règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 précité » et les mots : « s'assurer » sont remplacés par le mot : « garantir » ;

⑧ *b)* Au deuxième alinéa, après le mot : « négociation, », il est inséré le mot : « afin ».

Article 45

(Non modifié)

① Le code monétaire et financier est ainsi modifié :

② 1° À l'article L. 421-4, les mots : « aux alinéas 2 et 4 » sont remplacés par les mots : « au 2 » ;

③ 2° L'article L. 421-11 est ainsi modifié :

④ *a)* Le I est ainsi modifié :

⑤ – au 2, après le mot : « permettant », sont insérés les mots : « de gérer les risques auxquels elle est exposée, y compris les risques liés aux technologies de l'information et de la communication conformément au chapitre II du règlement (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, » ;

⑥ – le 4 est abrogé ;

⑦ *b)* À la seconde phrase du premier alinéa du III, les mots : « aux 2 et 4 » sont remplacés par les mots : « au 2 » et sont ajoutés les mots : « du présent article » ;

⑧ *c)* À la seconde phrase du second alinéa du même III, les mots : « aux 2 et 4 » sont remplacés par les mots : « au 2 » et, après la référence : « II », sont insérés les mots : « du présent article ».

Article 45 *bis*

① Le code monétaire et financier est ainsi modifié :

② 1° et 2° *(Supprimés)*

③ 3° *(nouveau)* Après l'article L. 621-9-3, il est inséré un article L. 621-9-4 ainsi rédigé :

④ « *Art. L. 621-9-4*. – I. – En application du premier alinéa du paragraphe 1 de l'article 19 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 , les entités financières soumises à ce règlement qui relèvent de la compétence de l'Autorité des marchés financiers adressent à l'Autorité des marchés financiers leurs déclarations d'incidents majeurs liés aux technologies de l'information et de la communication.

⑤ « Lorsque ces entités sont également soumises, en tant qu'entités essentielles ou importantes, aux dispositions de la directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) n° 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (directive SRI 2), elles transmettent également à l'autorité nationale de sécurité des systèmes d'information, en application du sixième alinéa du paragraphe 1 de l'article 19 du règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 précité, leurs déclarations

d'incidents majeurs liés aux technologies de l'information et de la communication.

⑥ « II. – En application du paragraphe 2 de l'article 19 du règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 précité, les entités financières mentionnées au premier alinéa du I du présent article peuvent adresser à l'Autorité des marchés financiers leurs notifications de cybermenaces. Dans ce cas, elles transmettent également ces notifications à l'autorité nationale de sécurité des systèmes d'information.

⑦ « III. – Les déclarations et notifications mentionnées aux I et II sont réalisées par le biais d'un document unique transmis simultanément à l'Autorité des marchés financiers et à l'autorité nationale de sécurité des systèmes d'information. » ;

⑧ 4° *(nouveau)* Après la douzième ligne du tableau du second alinéa du I des articles L. 783-8, L. 784-8 et L. 785-7, est insérée une ligne ainsi rédigée :

⑨

« L. 621-9-4	la loi n° du	».

Article 46

① L'article L. 511-41-1-B du code monétaire et financier est ainsi modifié :

② 1° Le deuxième alinéa est ainsi modifié :

③ *a)* Après le mot : « opérationnel, », sont insérés les mots : « dont les risques liés aux technologies de l'information et de la communication au sens 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, y compris ceux liés aux services de technologies de l'information et de la communication fournis par les prestataires tiers, » ;

④ *b)* Après le mot : « excessif », sont insérés les mots : « , les risques mis en évidence par des tests de résilience opérationnelle numérique prévus au chapitre IV du règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 précité » ;

⑤ 2° Le cinquième alinéa est ainsi modifié :

⑥ *a)* Après le mot : « établir », sont insérés les mots : « des politiques et » ;

⑦ *b)* Après le mot : « activité », sont insérés les mots : « ainsi que des plans de réponse et de rétablissement des technologies de l'information et de la communication concernant les technologies qu'ils utilisent pour la communication d'informations ».

Article 47

(Non modifié)

Au premier alinéa de l'article L. 511-55 du code monétaire et financier, après le mot : « saines, », sont insérés les mots : « de réseaux et de 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, ».

Article 48

(Non modifié)

① L'article L. 521-9 du code monétaire et financier est complété par un alinéa ainsi rédigé :

② « Ils respectent en outre les exigences prévues 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 applicables aux prestataires de services de paiement définis au I de l'article L. 521-1 du présent code. »

Article 49

(Non modifié)

① L'article L. 521-10 du code monétaire et financier est ainsi modifié :

② 1° Les I et II sont ainsi rédigés :

③ « I. – Les prestataires de services de paiement déclarent à l'Autorité de contrôle prudentiel et de résolution tout incident majeur, opérationnel ou de sécurité, lié au paiement. Les prestataires de services de paiement mentionnés au I de l'article L. 521-1 réalisent cette déclaration conformément à l'article 23 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.

④ « Lorsque les prestataires de services de paiement déclarent ces incidents à l'Autorité de contrôle prudentiel et de résolution, ils le font dans les conditions prévues à l'article 19 du même règlement, à l'exception des entités mentionnées au II de l'article L. 521-1 du présent code.

⑤ « L'Autorité de contrôle prudentiel et de résolution prend, au besoin, des mesures appropriées, conformément à l'article 22 du règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 précité, à l'exception des mesures relatives aux entités mentionnées au II de l'article L. 521-1 du présent code.

⑥ « En application de l'article L. 631-1, l'Autorité de contrôle prudentiel et de résolution communique ces incidents et, le cas échéant, les mesures prises à la Banque de France aux fins de l'accomplissement par celle-ci de ses missions prévues à l'article L. 141-4.

⑦ « II. – La Banque de France évalue les incidents opérationnels ou de sécurité majeurs liés au paiement. Elle prend au besoin des mesures appropriées et en informe l'Autorité de contrôle prudentiel et de résolution en application de l'article L. 631-1. » ;

⑧ 2° Il est ajouté un VI ainsi rédigé :

⑨ « VI. – La Caisse des dépôts et consignations réalise les déclarations mentionnées au I dans les conditions prévues par le décret en Conseil d'État mentionné à l'article L. 518-15-1. »

Article 49 *bis*

① Le III de l'article L. 532-50 du code monétaire et financier est complété par un alinéa ainsi rédigé :

② « 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 s'applique aux succursales agréées dans les conditions prévues au I du présent article dans les conditions prévues pour les succursales d'établissement de crédit agréées en application de l'article L. 511-10. »

Article 50

(Non modifié)

Au premier alinéa de l'article L. 533-2 du code monétaire et financier, après le mot : « informatiques », sont insérés les mots : « , y compris des réseaux et des 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, ».

Article 51

① L'article L. 533-10 du code monétaire et financier est ainsi modifié :

② 1° Le I est complété par un 6° ainsi rédigé :

③ « 6° Mettent en place des procédures administratives et comptables saines, des dispositifs de contrôle et de sauvegarde dans le domaine du traitement électronique des données, y compris des réseaux et des 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. Le présent 6° n'est pas applicable aux sociétés de gestion de portefeuille qui gèrent des fonds d'investissement alternatifs relevant du IV de l'article L. 532-9 ou des fonds d'investissement alternatifs relevant du I de l'article L. 214-167. » ;

④ 2° Le II est ainsi modifié :

⑤ *a)* À la première phrase du 4°, après le mot : « systèmes », sont insérés les mots : « appropriés et proportionnés, y compris des systèmes de

technologies de l'information et de la communication mis en place et gérés conformément à l'article 7 du règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 précité » ;

⑥ *b)* Le 5° est ainsi modifié :

⑦ – après le mot : « garantir », sont insérés les mots : « , conformément au même règlement, » ;

⑧ – après le mot : « information, », il est inséré le mot : « pour » ;

⑨ – après la dernière occurrence du mot : « et », il est inséré le mot : « pour ».

Article 52

① L'article L. 533-10-4 du code monétaire et financier est ainsi modifié :

② 1° Le *a* du 1° est complété par les mots : « , conformément aux exigences prévues 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 » ;

③ 2° Le 2° est ainsi modifié :

④ *a)* Le mot : « plans » est remplacé par le mot : « mécanismes » ;

⑤ *b)* Après le mot : « négociation, », sont insérés les mots : « 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 technologies de l'information et de la communication mis en place en application de l'article 11 du règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 précité » ;

⑥ *c)* Sont ajoutés les mots : « et aux chapitres II et IV du règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 précité ».

Article 53

(Suppression maintenue)

Article 54

① Le III de l'article L. 613-38 du code monétaire et financier est ainsi modifié :

② 1° Au 3°, après le mot : « continuité », sont insérés les mots : « et la résilience opérationnelle numérique » ;

③ 2° Le 17° est complété par les mots : « , y compris celui des réseaux et des systèmes d'information mentionnés dans 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 ».

Article 55

① Le quatrième alinéa du II de l'article L. 631-1 du code monétaire et financier est ainsi rédigé :

② « L'Autorité des marchés financiers, la Banque de France, l'Autorité de contrôle prudentiel et de résolution et l'autorité nationale de sécurité des systèmes d'information se communiquent sans délai les renseignements utiles à l'exercice de leurs missions respectives dans le domaine de la sécurité des systèmes d'information. »

Article 56

① Le code monétaire et financier est ainsi modifié :

② 1° Le I de l'article L. 712-7 est complété par un 15° ainsi rédigé :

③ « 15° 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. » ;

④ 2° La deuxième ligne du tableau du second alinéa du I des articles L. 752-10, L. 753-10 et L. 754-8 est ainsi rédigée :

⑤

«	L. 314-1	la loi n° du » ;

⑥ 3° *(Supprimé)*

⑦ 4° La quatrième ligne du tableau du second alinéa du I des articles L. 762-3, L. 763-3 et L. 764-3 est remplacée par deux lignes ainsi rédigées :

⑧

«	L. 420-3	la loi n° du
	L. 420-4 et L. 420-5	l'ordonnance n° 2017-1107 du 22 juin 2017 » ;

⑨ 5° Le tableau du second alinéa du I des articles L. 762-4, L. 763-4 et L. 764-4 est ainsi modifié :

⑩ *a)* La quatrième ligne est remplacée par trois lignes ainsi rédigées :

⑪

«	L. 421-3	l'ordonnance n° 2016-827 du 23 juin 2016
	L. 421-4	la loi n° du
	L. 421-5 à L. 421-7-2	l'ordonnance n° 2016-827 du 23 juin 2016 » ;

⑫ *b)* La dixième ligne est ainsi rédigée :

⑬

«	L. 421-11	la loi n° du » ;

⑭ 6° *(Supprimé)*

⑮ 7° La neuvième ligne du tableau du second alinéa du I des articles L. 773-5, L. 774-5 et L. 775-5 est remplacée par deux lignes ainsi rédigées :

⑯

«	L. 511-41-1-B	la loi n° du
	L. 511 41-1-C	l'ordonnance n° 2020-1635 du 21 décembre 2020 » ;

⑰ 8° La septième ligne du tableau du second alinéa du I des articles L. 773-6, L. 774-6 et L. 775-6 est ainsi rédigée :

⑱

«	L. 511-55	la loi n° du » ;

⑲ 9° La dernière ligne du tableau du second alinéa du I des articles L. 773-21, L. 774-21 et L. 775-15 est ainsi rédigée :

⑳

«	L. 521-9 et L. 521-10	la loi n° du		» ;

㉑ 9° *bis (nouveau)* La dix-septième ligne du tableau du second alinéa du I des articles L. 773-29, L. 774-29 et L. 775-23 est ainsi rédigée :

«	L. 532-50	la loi n° du		» ;

㉒ 10° Le tableau du second alinéa du I des articles L. 773-30, L. 774-30 et L. 775-24 est ainsi modifié :

㉓ *a)* La troisième ligne est ainsi rédigée :

㉔

«	L. 533-2	la loi n° du		» ;

㉕ *b)* La quatorzième ligne est ainsi rédigée :

㉖

«	L. 533-10	la loi n° du		» ;

㉗ *c)* La seizième ligne est remplacée par trois lignes ainsi rédigées :

㉘

«	L. 533-2 et L. 533-3	l'ordonnance n° 2016-827 du 23 juin 2016		
	L. 533-10-4	la loi n° du		
	L. 533-10-5 à L. 533-10-8	l'ordonnance n° 2016-827 du 23 juin 2016		» ;

㉙ 11° *(Supprimé)*

㉚ 12° La vingt et unième ligne du tableau du second alinéa du I des articles L. 783-4, L. 784-4 et L. 785-3 est ainsi rédigée :

㉛

«	L. 613-38	la loi n° du		» ;

㉜ 13° La deuxième ligne du tableau du second alinéa du I des articles L. 783-13, L. 784-13 et L. 785-12 est ainsi rédigée :

㉝

«	L. 631-1	la loi n° du		»

CHAPITRE II

Dispositions modifiant le code des assurances

Article 57

① L'article L. 354-1 du code des assurances est ainsi modifié :

② 1° À la première phrase du troisième alinéa, la dernière occurrence du mot : « à » est remplacée par les mots : « au 13° de » ;

③ 2° La seconde phrase de l'avant-dernier alinéa est complétée par les mots : « et elles mettent en place et gèrent des réseaux et des systèmes d'information en application 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 ».

Article 58

① Le I de l'article L. 356-18 du code des assurances est ainsi modifié :

② 1° À la première phrase du troisième alinéa, la dernière occurrence du mot : « à » est remplacée par les mots : « au 13° de » ;

③ 2° La seconde phrase du dernier alinéa est complétée par les mots : « et elles mettent en place et gèrent des réseaux et des systèmes d'information en application 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 ».

Article 58 *bis*

① Le code des assurances est ainsi modifié :

② 1° Le second alinéa de l'article L. 121-8 est remplacé par trois alinéas ainsi rédigés :

③ « Lorsque ces risques ne sont pas couverts par le contrat :

④ « 1° L'assuré doit prouver que le sinistre résulte d'un fait autre que le fait de guerre étrangère. Toutefois, lorsque le sinistre résulte d'une atteinte à

un système de traitement automatisé de données au sens des articles 323-1 à 323-8 du code pénal, il appartient à l'assureur de prouver qu'il résulte d'une guerre étrangère ;

⑤ « 2° Il appartient à l'assureur de prouver que le sinistre résulte d'une guerre civile, d'émeutes ou de mouvements populaires. » ;

⑥ 2° *(nouveau)* Après le troisième alinéa de l'article L. 194-1, il est inséré un alinéa ainsi rédigé :

⑦ « L'article L. 121-8 est applicable dans les îles Wallis et Futuna dans sa rédaction résultant de la loi n° du relative à la résilience des infrastructures critiques et au renforcement de la cybersécurité.»

CHAPITRE III

Dispositions modifiant le code de la mutualité

Article 59

La seconde phrase de l'avant-dernier alinéa de l'article L. 211-12 du code de la mutualité est complétée par les mots : « et elles mettent en place et gèrent des réseaux et des systèmes d'information en application 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 ».

Article 60

(Non modifié)

Le deuxième alinéa de l'article L. 212-1 du code de la mutualité est complété par les mots : « du présent code, à l'exception de l'article L. 354-1 du code des assurances ».

CHAPITRE IV

Dispositions modifiant le code de la sécurité sociale

Article 61

La seconde phrase de l'avant-dernier alinéa de l'article L. 931-7 du code de la sécurité sociale est complétée par les mots : « et elles mettent en place et gèrent des réseaux et des systèmes d'information en application 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 ».

CHAPITRE V

Dispositions finales

Article 62 A

Les entités financières essentielles et importantes auxquelles s'applique le présent titre et auxquelles s'impose, en application 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, l'adoption de mesures de gestion des risques en matière de cybersécurité ou la notification d'incidents importants ne sont pas tenues de se conformer aux exigences prévues par la directive (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), y compris celles relatives à la supervision, si l'adoption de ces mesures et la notification de ces incidents ont un effet au moins équivalent à ces exigences. Le présent article est applicable en Nouvelle-Calédonie, en Polynésie française et dans les îles Wallis et Futuna.

Article 62

① Le présent titre entre en vigueur le lendemain de la promulgation de la présente loi. Toutefois, les articles 46, 47 et 54 ne 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 modifiant le règlement (UE) n° 648/2012 qu'à compter du 17 janvier 2027.

② Lorsqu'elles remplissent les conditions prévues au même point 145, les sociétés de financement appliquent les règles énoncées aux chapitres II à IV et à la section 1 du chapitre V du règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 précité conformément au principe de proportionnalité énoncé à l'article 4 du même règlement.

③ Le présent article est applicable en Nouvelle-Calédonie, en Polynésie française et dans les îles Wallis et Futuna.

Article 63 ***(nouveau)***

Dans un délai de six mois à compter de la promulgation de la présente loi, le Gouvernement remet au Parlement un rapport présentant les moyens humains et financiers supplémentaires indispensables pour que l'autorité nationale de sécurité des systèmes d'information puisse contrôler l'application et l'effectivité de la présente loi.

Article 64 ***(nouveau)***

À compter de 2026, tous les ans, le Gouvernement remet au Parlement, avant le 30 septembre, un rapport sur la mise en œuvre de la stratégie nationale en matière de cybersécurité, qui précise les moyens humains, techniques et financiers mis à sa disposition pour l'exercice de ses missions de contrôle et d'audit. Il évalue également les besoins à venir au regard de l'élargissement du périmètre des entités concernées par la présente loi.