**RÉPUBLIQUE FRANÇAISE**

Ministère de l'économie, des finances, et de l'industrie

Ministère de l'enseignement supérieur et de la recherche

Intelligence artificielle et numérique

**TEXTE SOUMIS A LA DELIBERATION DU CONSEIL DES MINISTRES**

# Projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité

NOR : PRMD2412608L/Bleue-1

## TITRE Ier
## RESILIENCE DES ACTIVITES D'IMPORTANCE VITALE

### CHAPITRE Ier
### DISPOSITIONS GENERALES

### Article 1er

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

1° L'intitulé du chapitre est remplacé par l'intitulé suivant : « Résilience des activités d'importance vitale » ;

2° La section 1 est remplacée par les dispositions suivantes :

*« Section 1*
***« Dispositions générales relatives aux activités d'importance vitale***

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

« 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 ;

« 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 ;

« Parmi les infrastructures critiques, on distingue notamment :

« – les points d'importance vitale, c'est-à-dire les installations les plus sensibles, notamment celles qui sont difficilement substituables ;

« – les systèmes d'information d'importance vitale, c'est-à-dire les systèmes d'information nécessaires à l'exercice d'une activité d'importance vitale ou à la gestion, l'utilisation ou la protection d'une ou plusieurs infrastructures critiques ;

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

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

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

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

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

« 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.

*« Sous-section 1*
*« Dispositions applicables aux opérateurs d'importance vitale*

« *Art. L. 1332-3.* – Les opérateurs d'importance vitale réalisent une analyse des risques de toute nature, y compris à caractère terroriste, qui pourraient perturber l'exercice de leurs activités d'importance vitale ou la sécurité de leurs infrastructures critiques, notamment des points d'importance vitale désignés par l'autorité administrative.

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

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

« L'analyse des risques ainsi que les mesures de résilience sont détaillées dans un document dénommé "plan de résilience opérateur" élaboré par l'opérateur, au plus tard dans un délai de dix mois à compter de la désignation prévue au I de l'article L. 1332-2, et approuvé par l'autorité administrative.

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

« En cas de refus de l'opérateur d'élaborer ce plan, de le modifier afin de le rendre conforme aux exigences prévues au présent article ou de le mettre en œuvre, l'autorité administrative le met en demeure de le réaliser, de le modifier ou de le mettre en œuvre dans un délai qu'elle fixe et qui ne saurait être inférieur à un mois.

« L'autorité administrative peut assortir cette mise en demeure d'une astreinte d'un montant maximal de 5 000 euros par jour de retard.

« L'astreinte peut également être prononcée à tout moment, après l'expiration du délai imparti par la mise en demeure, s'il n'y a pas été satisfait, après que l'intéressé a été invité à présenter ses observations.

« 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$^{er}$ du livre V du code de l'environnement et des dispositions du chapitre III du titre IX du livre V du même code.

« Un décret en Conseil d'Etat précise la nature des mesures de résilience pour chaque catégorie d'opérateur d'importance vitale mentionnée au I de l'article L. 1332-2.

« *Art. L. 1332-4.* – Les opérateurs d'importance vitale réalisent, au plus tard dans un délai de neuf mois à compter de la désignation prévue au I de l'article L. 1332-2, une analyse de leurs dépendances à l'égard de tiers, y compris ceux situés en dehors du territoire national, pour l'exercice de leurs activités d'importance vitale. Celle-ci comprend notamment une analyse des éventuelles vulnérabilités de leurs chaînes d'approvisionnement. Les mesures de résilience adoptées par les opérateurs d'importance vitale tiennent compte de cette analyse.

« Les opérateurs d'importance vitale prennent les mesures nécessaires pour garantir l'application des dispositions prévues au présent chapitre.

« *Art. L. 1332-5.* – Les opérateurs dont un ou plusieurs points d'importance vitale sont désignés en application du présent chapitre réalisent pour chacun d'eux un document dénommé "plan particulier de résilience" détaillant les mesures de protection et de résilience les concernant.

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

« Lorsque, en application d'accords internationaux régulièrement ratifiés ou approuvés, de lois ou de règlements, un point d'importance vitale fait déjà l'objet de mesures de protection suffisantes décrites dans un document particulier, l'autorité administrative peut décider que ce document tient lieu de "plan particulier de résilience".

« En cas de refus de l'opérateur d'élaborer ce plan, de le modifier afin de le rendre conforme aux exigences prévues aux alinéas précédents ou de le mettre en œuvre, l'autorité administrative le met en demeure de le réaliser, de le modifier ou de le mettre en œuvre dans un délai qu'elle fixe et qui ne saurait être inférieur à un mois.

« L'autorité administrative peut assortir cette mise en demeure d'une astreinte d'un montant maximal de 5 000 euros par jour de retard.

« L'astreinte peut également être prononcée à tout moment, après l'expiration du délai imparti par la mise en demeure, s'il n'y a pas été satisfait, après que l'opérateur concerné a été invité à présenter ses observations.

« *Art. L. 1332-6.* – Avant d'accorder une autorisation d'accès physique ou à distance à ses points d'importance vitale et systèmes d'information d'importance vitale, l'opérateur d'importance vitale peut demander l'avis de l'autorité administrative compétente dans les conditions prévues par l'article L. 114-1 du code de la sécurité intérieure, selon des modalités fixées par décret en Conseil d'Etat, lorsqu'il estime nécessaire de s'assurer que le comportement de la personne devant faire l'objet de l'autorisation d'accès n'est pas de nature à porter atteinte à l'exercice d'une activité d'importance vitale ou à la sécurité d'une infrastructure critique.

« Il peut également solliciter cet avis avant le recrutement ou l'affectation d'une personne à un poste pour l'exercice duquel il est nécessaire d'avoir accès aux points d'importance vitale ou aux systèmes d'information d'importance vitale ou qui implique l'occupation de fonctions sensibles.

« Les fonctions sensibles sont celles qui sont indispensables à la réalisation d'une activité d'importance vitale ou dont l'occupation expose l'opérateur à des vulnérabilités. Elles sont énumérées par l'opérateur dans le plan de résilience prévu au quatrième alinéa de l'article L. 1332-3 en tenant compte, le cas échéant, de critères déterminés par l'autorité administrative en fonction du secteur d'activité de l'opérateur.

« Les cas dans lesquels les accès physiques ou à distance peuvent justifier la demande d'avis sont précisés par l'opérateur dans le plan de résilience prévu au quatrième alinéa de l'article L. 1332-3 et, le cas échéant, dans le plan particulier de résilience prévu à l'article L. 1332-5 en tenant compte des vulnérabilités à des actes de malveillance.

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

« En cas d'avis défavorable de l'autorité administrative, l'opérateur d'importance vitale est tenu de refuser l'autorisation s'il est une personne morale de droit privé. Un avis défavorable ne peut être émis que s'il ressort de l'enquête administrative que le comportement de la personne ayant fait l'objet de l'enquête est de nature à porter atteinte à l'exercice d'une activité d'importance vitale ou à la sécurité d'une infrastructure critique.

« *Art. L. 1332-7.* – Les opérateurs d'importance vitale désignés au titre du 1° du I de l'article L. 1332-2 notifient à l'autorité administrative tout incident susceptible de compromettre la continuité de ses activités d'importance vitale dans un délai prévu par décret en Conseil d'Etat.

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

*« Sous-section 2*
*« Dispositions applicables aux entités critiques d'importance européenne particulière*

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

« Ces opérateurs sont identifiés comme entités critiques d'importance européenne particulière de l'opérateur dans les conditions prévues à l'article 17 de la directive (UE) du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience des entités critiques, et abrogeant la directive 2008/114/CE du Conseil.

« Les opérateurs qui exercent des activités dans les domaines de la sécurité nationale, de la sécurité publique, de la défense, du nucléaire ou de la répression pénale, ou qui fournissent des services exclusivement destinés aux entités de l'administration publique exerçant dans ces domaines, peuvent être exonérés par l'autorité administrative de tout ou partie des obligations mentionnées à la présente sous-section, dans des conditions prévues par décret en Conseil d'Etat.

« *Art. L. 1332-9.* – Lorsque l'opérateur a été désigné par la Commission européenne comme entité critique d'importance européenne particulière il peut, avec l'accord de l'autorité administrative compétente, faire l'objet d'une mission de conseil au titre de laquelle il doit garantir l'accès aux informations, systèmes et installations relatifs à la fourniture de leurs services essentiels qui sont nécessaires à l'exécution de cette mission de conseil, dans le respect des secrets protégés par la loi.

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

3° La section 1 *bis* devient une sous-section 3 de la section 1 ;

4° L'article L. 1332-6-1 A devient l'article L. 1332-10, et, dans cet article, les mots : « mentionnés aux articles L. 1332-1 et L. 1332-2 » sont remplacés par les mots : « mentionnés au I de l'article L. 1332-2 » ;

5° Les sections 2 et 3 sont remplacées par les dispositions suivantes :

*« Sous-section 4*
*« Dispositions applicables aux systèmes d'information*

« *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 et 16 et au premier alinéa de l'article 17 de la loi n° ….. du ….. relative à la résilience des infrastructures critiques et au renforcement de la cybersécurité.

« II. – Pour répondre aux crises majeures menaçant ou affectant la sécurité des systèmes d'information, le Premier ministre peut décider des mesures que les opérateurs mentionnés au I de l'article L. 1332-2 doivent mettre en œuvre.

*« Section 2*
***« Contrôles et sanctions administratives***

*« Sous-section 1*
*« Habilitation et contrôles*

« *Art. L. 1332-12.* – Sont habilités à rechercher et constater les infractions et manquements aux prescriptions du présent chapitre, à l'exception de l'article L. 1332-11, ainsi qu'aux dispositions réglementaires prises pour son application, en vue de la saisine de la commission prévue à l'article L. 1332-15, les agents de l'Etat spécialement désignés et assermentés à cette fin dans des conditions précisées par décret en Conseil d'Etat.

« *Art. L. 1332-13.* – Les agents mentionnés à l'article L. 1332-12 ont accès, pour l'exercice de leurs missions, aux locaux des opérateurs d'importance vitale. Ils peuvent pénétrer dans les lieux à usage professionnel ou dans les lieux d'exécution d'une prestation de service.

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

« Ils peuvent recueillir, sur place ou sur convocation, tout renseignement, toute justification ou tout document nécessaire aux contrôles. A ce titre, ils peuvent exiger la communication de documents de toute nature propres à faciliter l'accomplissement de leur mission. Ils peuvent les obtenir ou en prendre copie, par tout moyen et sur tout support, ou procéder à la saisie de ces documents en quelques mains qu'ils se trouvent.

« Ils peuvent procéder, sur convocation ou sur place, aux auditions de toute personne susceptible d'apporter des éléments utiles à leurs constatations. Ils en dressent procès-verbal. Les personnes entendues procèdent elles-mêmes à sa lecture, peuvent y faire consigner leurs observations et y apposent leur signature. En cas de refus de signer le procès-verbal, mention en est faite sur celui-ci.

« Ils sont astreints au secret professionnel pour les faits, actes ou renseignements dont ils ont pu avoir connaissance en raison de leurs fonctions, dans les conditions prévues à l'article 226-13 du code pénal. Le secret professionnel ne peut leur être opposé.

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

« *Art. L. 1332-14.* – Il est interdit de faire obstacle à l'exercice des fonctions des agents habilités. L'opérateur contrôlé est tenu de coopérer avec l'autorité administrative. Les agents mentionnés à l'article L. 1332-12 peuvent constater toute action de l'opérateur d'importance vitale de nature à faire obstacle au contrôle.

« Le fait pour quiconque de faire obstacle aux demandes de l'autorité compétente nécessaires à la recherche des manquements et à la mise en œuvre de ses pouvoirs de contrôle prévus par la présente sous-section, notamment en fournissant des renseignements incomplets ou inexacts, ou en communiquant des pièces incomplètes ou dénaturées, est puni d'une amende administrative prononcée par la commission des sanctions mentionnée à l'article L. 1332-15 dont le montant, proportionné à la gravité du manquement, ne peut excéder dix millions d'euros ou, lorsqu'il s'agit d'une entreprise, 2 % du chiffre d'affaires annuel mondial, hors taxes, de l'exercice précédent, le montant le plus élevé étant retenu.

« Ces dispositions ne s'appliquent pas à l'Etat et à ses établissements publics administratifs qui font l'objet d'un contrôle.

*« Sous-section 2*
*« Sanctions*

« *Art. L. 1332-15.* – Tout manquement aux dispositions du présent chapitre peut donner lieu aux sanctions prévues à l'article L. 1332-17, prononcées par une commission des sanctions instituée à cet effet auprès du Premier ministre.

« Cette commission est saisie par l'autorité administrative des manquements constatés lors des contrôles effectués en application de l'article L. 1332-13. Cette autorité notifie à l'opérateur concerné les griefs susceptibles d'être retenus à son encontre.

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

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

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

« 2° Et de trois personnalités qualifiées nommées par le Premier ministre en raison de leurs compétences dans le domaine de la sécurité des activités d'importance vitale.

« Un suppléant est désigné dans les mêmes conditions pour les membres mentionnés au 1°.

« Les membres de la commission des sanctions exercent leurs fonctions en toute impartialité. Dans l'exercice de leurs attributions, ils ne reçoivent ni ne sollicitent d'instruction d'aucune autorité.

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

« La commission des sanctions statue par décision motivée. Aucune sanction ne peut être prononcée sans que l'opérateur concerné ou son représentant ait été entendu ou, à défaut, dûment convoqué. La commission peut auditionner toute personne qu'elle juge utile.

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

« Le président et les membres de la commission ainsi que leurs suppléants respectifs sont nommés par décret pour un mandat de cinq ans, renouvelable une fois. Ils sont tenus au secret professionnel.

« *Art. L. 1332-17.* – I. – En cas de manquement aux obligations découlant de l'application des dispositions du présent chapitre, la commission des sanctions peut prononcer à l'encontre des opérateurs d'importance vitale, à l'exception des administrations de l'Etat et de ses établissements publics administratifs, des collectivités territoriales, de leurs groupements et de leurs établissements publics administratifs, une amende administrative dont le montant, proportionné à la gravité du manquement, ne peut excéder dix millions d'euros ou, lorsqu'il s'agit d'une entreprise, 2 % du chiffre d'affaires annuel mondial, hors taxes, de l'exercice précédent, le montant le plus élevé étant retenu.

« Lorsque la commission des sanctions envisage également de prononcer la sanction prévue au deuxième alinéa de l'article L. 1332-14, le montant cumulé ne peut excéder le montant maximum prévu à l'alinéa précédent.

« II. – En cas de manquement constaté aux obligations découlant de l'application des dispositions mentionnées aux 1° à 5° de l'article 26 de la loi n° … 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 cette loi, peut prononcer les sanctions prévues à l'article 28 et à l'article 37 de la même loi.

« *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.

« Les sanctions pécuniaires sont versées au Trésor public et recouvrées comme créances de l'Etat étrangères à l'impôt et au domaine.

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

« *Art. L. 1332-19.* – Les conditions d'application de la présente sous-section, notamment les règles de fonctionnement de la commission et les modalités de récusation de ses membres, sont définies par décret en Conseil d'Etat.

*« Section 3*
***« Marchés publics et contrats de concession relatifs à la sécurité des activités d'importance vitale***

« *Art. L. 1332-20.* – 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 :

« – ces marchés publics concernent la conception, la qualification, la fabrication, la modification, la maintenance ou le retrait des structures, équipements, systèmes, matériels, composants ou logiciels nécessaires à la protection des infrastructures critiques de l'opérateur ou dont le détournement de l'usage porterait atteinte aux intérêts essentiels de l'Etat ;

« – et que cette protection ou la prévention de ce détournement d'usage ne peuvent être garanties par d'autres moyens.

« *Art. L. 1332-21.* – 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 :

« – ces contrats de concession concernent la conception, la qualification, la fabrication, la modification, la maintenance ou le retrait des structures, équipements, systèmes, matériels, composants ou logiciels nécessaires à la protection des infrastructures critiques de l'opérateur ou dont le détournement de l'usage porterait atteinte aux intérêts essentiels de l'Etat ;

« – et que cette protection ou la prévention de ce détournement d'usage ne peuvent être garanties par d'autres moyens.

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

## CHAPITRE II
## DISPOSITIONS DIVERSES

### Article 2

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

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 » ;

2° Au premier alinéa de l'article L. 2113-2, dans sa rédaction issue de l'article 47 de la loi n° 2023-703 du 1er août 2023 relative à la programmation militaire pour les années 2024 à 2030 et portant diverses dispositions intéressant la défense, 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 » ;

3° Au deuxième alinéa de l'article L. 2151-1, les mots : « , visé par un plan de continuité ou de rétablissement d'activité, d'un des opérateurs 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 : « 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 » ;

4° A 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 » ;

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 : « opérateurs d'importance vitale mentionnés au I de l'article L. 1332-2 » ;

6° Au premier et au quatrième alinéa 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 » ;

7° A l'article L. 2321-3 :

*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 du présent code » ;

*b)* Au 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 » ;

8° A l'article L. 4231-6, les mots : « publics et 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 : « opérateurs d'importance vitale mentionnés au I de l'article L. 1332-2 ».

II. – 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 ».

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

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 » ;

2° Au premier alinéa de l'article L. 33-14 et 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 ».

IV. – Au 2° du II et au 2° du 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 ».

V. – Le code de la sécurité intérieure est ainsi modifié :

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 » ;

2° Au 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 ».

VI. – 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

I. – La sixième partie du code de la défense est ainsi modifiée :

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

« *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. » ;

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

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

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

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

4° Le chapitre II du titre I$^{er}$ du livre III est complété par un article L. 6312-3 ainsi rédigé :

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

II. – A l'article 711-1 du code pénal, les mots : « loi n° 2024-247 du 21 mars 2024 renforçant la sécurité et la protection des maires et des élus locaux » sont remplacés par les mots : « loi n° ….. du ….. relative à la résilience des infrastructures critiques et au renforcement de la cybersécurité ».

III. – Le chapitre II du titre I$^{er}$ du livre II du code des postes et des communications électroniques est ainsi modifié :

1° Au 1° du VII de l'article L. 33-1, les mots : « l'ordonnance n° 2021-650 du 26 mai 2021 portant transposition de la directive (UE) 2018/1972 du Parlement européen et du Conseil du 11 décembre 2018 établissant le code des communications électroniques européen et relative aux mesures d'adaptation des pouvoirs de l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse » sont remplacés par les mots : « la loi n° ….. du ….. relative à la résilience des infrastructures critiques et au renforcement de la cybersécurité » ;

2° A l'article L. 33-15, les mots : « loi n° 2023-703 du 1$^{er}$ août 2023 relative à la programmation militaire pour les années 2024 à 2030 et portant diverses dispositions intéressant la défense » sont remplacés par les mots : « loi n° ….. du ….. relative à la résilience des infrastructures critiques et au renforcement de la cybersécurité » ;

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 ».

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 : « loi n° 2023-703 du 1er août 2023 relative à la programmation militaire pour les années 2024 à 2030 et portant diverses dispositions intéressant la défense » sont remplacés par les mots : « loi n° ….. du ….. relative à la résilience des infrastructures critiques et au renforcement de la cybersécurité ».

## CHAPITRE III
## DISPOSITIONS TRANSITOIRES

### Article 4

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

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

# TITRE II
# CYBERSÉCURITÉ

## CHAPITRE Ier
## DE L'AUTORITE NATIONALE DE SECURITE DES SYSTEMES D'INFORMATION

### Article 5

L'autorité nationale de sécurité des systèmes d'information est chargée de la mise en œuvre de la politique du Gouvernement en matière de sécurité des systèmes d'information régie par le présent titre et de son contrôle.

Le Premier ministre peut désigner un organisme autre que l'autorité nationale de sécurité des systèmes d'information mentionnée au premier alinéa pour exercer à l'égard de certaines entités, à raison de leur activité dans le domaine de la défense, certaines des responsabilités de cette autorité prévues par le présent titre.

Les missions de l'autorité nationale et des organismes désignés par le Premier ministre ainsi que leurs conditions d'exercice sont précisées par décret en Conseil d'Etat.

## CHAPITRE II
## DE LA CYBER RESILIENCE

### Section 1
### Définitions

### Article 6

Au sens du présent titre, on entend par :

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

2° Office d'enregistrement : une entité à laquelle un domaine de premier niveau spécifique a été délégué et qui est responsable de l'administration de ce domaine, y compris de l'enregistrement des noms de domaine en relevant et de son fonctionnement technique, notamment l'exploitation de ses serveurs de noms, la maintenance de ses bases de données et la distribution de ses fichiers de zone sur les serveurs de noms, que ces opérations soient effectuées par l'entité elle-même ou qu'elles soient sous-traitées, mais à l'exclusion des situations où les noms de domaine de premier niveau sont utilisés par un registre uniquement pour son propre usage ;

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 ;

4° Prestataire de service de confiance qualifié : un prestataire de services de confiance au sens du paragraphe 20 de l'article 3 du règlement (UE) n° 910/2014 mentionné ci-dessus ;

5° Représentant : une personne physique ou morale établie dans l'Union qui est expressément désignée pour agir pour le compte d'un fournisseur de services de système de nom de domaine, d'un registre de noms de domaine de premier niveau, d'une entité fournissant des services d'enregistrement de noms de domaine, d'un fournisseur d'informatique en nuage, d'un fournisseur de services de centre de données, d'un fournisseur de réseau de diffusion de contenu, d'un fournisseur de services gérés, d'un fournisseur de services de sécurité gérés ou d'un fournisseur de places de marché en ligne, de moteurs de recherche en ligne ou de plateformes de services de réseaux sociaux non établi dans l'Union, qui peut être contactée par une autorité compétente ou un centre de veille, d'alerte et de réponse aux attaques informatiques (CERT) à la place de l'entité elle-même concernant les obligations incombant à ladite entité en vertu de la présente loi ;

6° Service de centre de données : un service qui englobe les structures, ou groupes de structures, dédiées à l'hébergement, l'interconnexion et l'exploitation centralisées des équipements informatiques et de réseau fournissant des services de stockage, de traitement et de transport des données, ainsi que l'ensemble des installations et infrastructures de distribution d'électricité et de contrôle environnemental ;

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

Section 2
**Des exigences de sécurité des systèmes d'information**

**Article 7**

La liste des secteurs d'activité critiques et hautement critiques pour le fonctionnement de l'économie et de la société mentionnés dans la présente section est fixée par décret en Conseil d'Etat.

**Article 8**

Sont des entités essentielles :

1° Les entreprises appartenant à un des secteurs d'activité hautement critiques qui emploient au moins 250 personnes ou dont le chiffre d'affaires annuel excède 50 millions d'euros et dont le total du bilan annuel excède 43 millions d'euros ;

2° Les établissements publics à caractère industriel et commercial, à l'exception du Commissariat à l'énergie atomique et aux énergies alternatives pour ses seules activités dans le domaine de la défense, ainsi que les régies dotées de la seule autonomie financière chargées d'un service public industriel et commercial créées en application du 2° de l'article L. 2221-4 du code général des collectivités territoriales, appartenant à un des secteurs d'activité hautement critiques, qui emploient au moins 250 personnes ou dont les produits d'exploitation excèdent 50 millions d'euros et le total du bilan annuel excède 43 millions d'euros. Le critère d'emploi est calculé selon les modalités prévues par le I de l'article L. 130-1 du code de la sécurité sociale, les critères financiers sont appréciés au niveau de la personne morale ou de la régie concernée ;

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

4° Les prestataires de service de confiance qualifiés ;

5° Les offices d'enregistrement ;

6° Les fournisseurs de services de système de noms de domaine ;

7° Les administrations suivantes :

*a)* Les administrations de l'Etat et leurs établissements publics administratifs, à l'exception des administrations de l'Etat qui exercent leurs activités dans les domaines de la sécurité publique, de la défense et de la sécurité nationale, de la répression pénale et des missions diplomatiques et consulaires françaises pour leurs réseaux et systèmes d'information ainsi que de leurs établissements publics administratifs qui exercent leurs activités dans les mêmes domaines ou qui sont désignés entité importante par arrêté du Premier ministre. Le Premier ministre désigne par arrêté les établissements publics administratifs de l'Etat qui, compte tenu du faible impact économique et social de leur activité, ne sont pas soumis à la présente loi, dans des conditions précisées par décret en Conseil d'Etat ;

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

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

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

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

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

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

*h)* Et les autres organismes et personnes de droit public ou de droit privé chargés d'une mission de service public administratif, mentionnés au 1° de l'article L. 100-3 du code des relations entre le public et l'administration, à compétence nationale, à l'exception de ceux qui sont désignés entité importante par arrêté du Premier ministre. Le Premier ministre désigne par arrêté les organismes et personnes morales qui, compte tenu du faible impact économique et social de leur activité, ne sont pas soumis à la présente loi, dans des conditions précisées par décret en Conseil d'Etat ;

8° Les opérateurs d'importance vitale en tant qu'ils exercent une activité qualifiée de service essentiel en application du deuxième alinéa du 1° du I de l'article L. 1332-2 du code de la défense ;

9° Les opérateurs de services essentiels désignés en application des dispositions de l'article 5 de la loi n° 2018-133 du 26 février 2018 portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité avant l'entrée en vigueur de la présente loi ;

10° Les établissements d'enseignement menant des activités de recherche désignés par arrêté du Premier ministre dans des conditions précisées par décret en Conseil d'Etat, qui remplissent l'un des critères mentionnés à l'article 10.

**Article 9**

Sont des entités importantes :

1° Les entreprises appartenant à un des secteurs d'activité hautement critiques ou critiques qui ne sont pas des entités essentielles et qui emploient au moins 50 personnes ou dont le chiffre d'affaires et le total du bilan annuel excèdent chacun 10 millions d'euros ;

2° Les opérateurs de communications électroniques qui ne sont pas des entités essentielles ;

3° Les prestataires de services de confiance qui ne sont pas des entités essentielles ;

4° Les communautés de communes et leurs établissements publics administratifs dont les activités s'inscrivent dans un des secteurs d'activité hautement critiques ou critiques ;

5° Les établissements d'enseignement menant des activités de recherche qui ne sont pas des entités essentielles. Le Premier ministre désigne par arrêté les établissements qui, compte tenu du faible impact économique et social de leur activité, ne sont pas soumis à la présente loi, dans les conditions précisées par décret en Conseil d'Etat ;

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

7° Les autres organismes et personnes de droit public ou de droit privé chargés d'une mission de service public administratif, mentionnés au 1° de l'article L. 100-3 du code des relations entre le public et l'administration, à compétence nationale, expressément désignés en tant qu'entités importantes par arrêté du Premier ministre dans les conditions précisées par décret en Conseil d'Etat ;

8° Les établissements publics à caractère industriel et commercial et les régies dotées de la seule autonomie financière chargées d'un service public industriel et commercial créées en application du 2° de l'article L. 2221-4 du code général des collectivités territoriales, relevant des secteurs d'activité hautement critiques ou critiques, qui emploient au moins 50 personnes ou dont le produit d'exploitation et le total du bilan annuel excèdent chacun 10 millions d'euros et qui ne sont pas entités essentielles. Le critère d'emploi est calculé selon les modalités prévues par le I de l'article L. 130-1 du code de la sécurité sociale, les critères financiers sont appréciés au niveau de la personne morale ou de la régie concernée.

**Article 10**

Outre les entités mentionnées aux articles 8 et 9, le Premier ministre peut désigner par arrêté comme entité essentielle ou comme entité importante une entité exerçant une activité relevant d'un secteur d'activité hautement critique ou critique, quelle que soit sa taille, sous réserve de justifier cette désignation au regard de l'un des critères suivants :

1° L'entité est le seul prestataire sur le territoire national d'un service qui est essentiel au maintien du fonctionnement de la société et d'activités économiques critiques ;

2° Une perturbation du service fourni par l'entité pourrait avoir un impact important sur la sécurité publique, la sûreté publique ou la santé publique ;

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

4° L'entité est critique en raison de son importance spécifique au niveau national ou local pour le secteur ou le type de service concerné, ou pour d'autres secteurs interdépendants sur le territoire national.

**Article 11**

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

1° Elles sont établies sur le territoire national ;

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

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

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

*b)* Ou, s'ils sont établis hors de l'Union européenne mais offrent leurs services sur le territoire national, ils ont désigné un représentant établi sur le territoire national.

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

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

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

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.

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

**Article 12**

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

Les informations à transmettre, leurs modalités de communication et les délais dans lesquels les modifications doivent être transmises sont définis par décret en Conseil d'Etat.

**Article 13**

Les dispositions pertinentes de la présente loi, y compris celles relatives à la supervision, ne sont pas applicables aux entités essentielles et importantes qui sont soumises, en application d'un acte juridique de l'Union européenne, à des exigences sectorielles de sécurité et de notification d'incidents ayant un effet au moins équivalent aux obligations résultant des articles 14 et 17. Pour être équivalentes, les exigences de notification des incidents doivent également prévoir un accès immédiat aux notifications d'incidents par l'autorité nationale de sécurité des systèmes d'information.

**Article 14**

Les entités essentielles, les entités importantes, les administrations de l'Etat et leurs établissements publics administratifs qui exercent leurs activités dans les domaines de la sécurité publique, de la défense et de la sécurité nationale ainsi que de la répression pénale, les missions diplomatiques et consulaires françaises pour leurs réseaux et systèmes d'information, le Commissariat à l'énergie atomique et aux énergies alternatives pour ses activités dans le domaine de la défense ainsi que les juridictions administratives et judiciaires prennent les mesures techniques, opérationnelles et organisationnelles appropriées et proportionnées pour gérer les risques qui menacent la sécurité des réseaux et des systèmes d'information qu'elles utilisent dans le cadre de leurs activités ou de la fourniture de leurs services, ainsi que pour éliminer ou réduire les conséquences que les incidents ont sur les destinataires de leurs services et sur d'autres services. Ces mesures garantissent, pour leurs réseaux et leurs systèmes d'information, un niveau de sécurité adapté et proportionné au risque existant. Elles visent à :

1° Mettre en place un pilotage de la sécurité des réseaux et systèmes d'information adaptée, comprenant notamment la formation à la cybersécurité des membres des organes de direction et des personnes exposées aux risques ;

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

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

4° Garantir la résilience des activités.

Un décret en Conseil d'Etat fixe les objectifs auxquels doivent se conformer les personnes mentionnées au premier alinéa afin que les mesures adoptées pour la gestion des risques satisfassent aux 1° à 4°. Ce décret détermine également les conditions d'élaboration, de modification et de publication d'un référentiel d'exigences techniques et organisationnelles qui sont adaptées aux différentes personnes mentionnées au premier alinéa.

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) nº 526/2013.

Par dérogation aux deux alinéas précédents, les fournisseurs de services de systèmes de noms de domaine, les offices d'enregistrement, les fournisseurs de services d'informatique en nuage, les fournisseurs de services de centres de données, les fournisseurs de réseaux de diffusion de contenu, les fournisseurs de services gérés, les fournisseurs de services de sécurité gérés, ainsi que les fournisseurs de places de marché en ligne, de moteurs de recherche en ligne et de plateformes de services de réseaux sociaux, et les prestataires de services de confiance mettent en œuvre les exigences techniques et méthodologiques qui leur sont propres.

Ces mesures techniques, opérationnelles et organisationnelles sont mises en œuvre aux frais des personnes concernées.

**Article 15**

Les personnes mentionnées à l'article 14 qui mettent en œuvre les exigences du référentiel mentionné au sixième alinéa du même article 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 même alinéa.

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**

Les opérateurs mentionnés à l'article L. 1332-2 du code de la défense identifient, 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 2° de l'article L. 1332-1 du même code selon les modalités fixées par le Premier ministre.

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

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

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

**Article 17**

Les personnes mentionnées à l'article 14 notifient sans retard injustifié à l'autorité nationale de sécurité des systèmes d'information tout incident ayant un impact important sur la fourniture de leurs services.

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.

Les entités essentielles et importantes notifient sans délai aux destinataires de leurs services :

1° Les incidents critiques susceptibles de nuire à la fourniture de ces services ;

2° Les vulnérabilités critiques affectant leurs services ou les affectant potentiellement, ainsi que les mesures ou corrections, dès qu'elles en ont connaissance, que ces destinataires peuvent appliquer en réponse à cette vulnérabilité ou à cette menace.

Cette obligation de notification ne s'étend pas aux informations dont la divulgation porterait atteinte aux intérêts de la défense et de la sécurité nationale.

En cas d'incident critique ou de vulnérabilité critique, les personnes mentionnées au premier alinéa 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.

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 susceptible d'entraîner une violation de données à caractère personnel.

Un décret en Conseil d'Etat fixe les modalités d'application du présent article. Il précise notamment la procédure applicable et les critères d'appréciation des caractères importants et critiques des incidents et vulnérabilités ainsi que les délais de notification des incidents et des vulnérabilités.

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 satisfont à l'une des conditions prévues à l'article 11 sont soumis aux dispositions de la présente section.

**Article 19**

Les offices d'enregistrement collectent, par l'intermédiaire des bureaux d'enregistrement ainsi que des agents agissant pour le compte de ces derniers, les données nécessaires à l'enregistrement des noms de domaine.

Les offices et les bureaux d'enregistrement sont responsables du traitement de ces données au regard de la réglementation en matière de protection des données personnelles. Ils tiennent ces bases de données à jour, en maintenant les données exactes et complètes, sans redondance de collecte. A cette fin, ils mettent en place des procédures, accessibles au public, permettant de vérifier ces données lors de leur collecte et d'assurer la sécurité de leur base de données.

Un décret en Conseil d'Etat, pris après avis de la Commission nationale informatique et libertés, fixe la liste des données relatives aux noms de domaine devant être collectées.

**Article 20**

Les offices et les bureaux d'enregistrement conservent les données relatives à chaque nom de domaine dans leur base de données tant que le nom de domaine est utilisé.

### Article 21

Les offices et bureaux d'enregistrement rendent publiques sans retard injustifié après l'enregistrement d'un nom de domaine, les données d'enregistrement relatives à ce nom de domaine dès lors qu'elles n'ont pas de caractère personnel.

### Article 22

Pour les besoins des procédures pénales et de la sécurité des systèmes d'information, les agents habilités à cet effet par l'autorité judiciaire ou par l'autorité nationale de sécurité des systèmes d'information peuvent obtenir des offices et bureaux d'enregistrement les données mentionnées à l'article 20.

Les offices et les bureaux d'enregistrement fixent les règles de procédure pour la communication de ces données aux agents mentionnés au premier alinéa. Cette communication intervient dans un délai n'excédant pas soixante-douze heures. Ces règles sont accessibles au public.

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

## Section 4
## Coopération et échange d'informations

### Article 23

Les dispositions de l'article 11 du code de procédure pénale ou celles relatives aux autres secrets protégés par la loi ne font pas obstacle à la communication d'informations dont ils disposent aux fins de l'accomplissement de leurs missions respectives, à l'exception des informations dont la communication porterait atteinte à la sécurité publique, à la défense et la sécurité nationale ou à la conduite des relations internationales, entre, d'une part, l'autorité nationale de sécurité des systèmes d'information, et, d'autre part, la Commission nationale de l'informatique et des libertés ou les autorités compétentes chargées de la gestion des risques en matière de cybersécurité en vertu d'un acte sectoriel de l'Union européenne ou les autorités chargées de la conduite de la politique pénale, de l'action publique et de l'instruction ou la Commission européenne ou les autorités compétentes des autres Etats membres de l'Union européenne ou des centres de réponse aux incidents de sécurité informatique ou des organismes internationaux concourant aux missions de sécurité ou de défense des systèmes d'information.

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

### Article 24

L'autorité nationale de sécurité des systèmes d'information agrée des organismes publics ou privés en tant que relais dans la prévention et la gestion des incidents. L'autorité et les organismes qu'elle a ainsi agréés sont autorisés à échanger entre eux des informations couvertes par des secrets protégés par la loi.

Les modalités d'application du présent article, notamment les modalités de dépôt et d'examen des demandes d'agrément des organismes mentionnés au premier alinéa, sont déterminées par décret en Conseil d'Etat.

## CHAPITRE III
## DE LA SUPERVISION

### Article 25

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 et des bureaux d'enregistrement, l'autorité nationale de sécurité des systèmes d'information peut prescrire à la personne ou au bureau d'enregistrement concerné les mesures nécessaires, notamment pour éviter un incident ou y remédier, ainsi que les délais pour mettre en œuvre ces mesures et en rendre compte.

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

### Section 1
### Recherche et constatations des manquements

#### Sous-section 1
#### Habilitation

### Article 26

Les agents et personnes, spécialement désignés et assermentés à cet effet, de l'autorité nationale de sécurité des systèmes d'information, des organismes indépendants ou d'autres services de l'Etat qu'elle désigne sont habilités à rechercher et à constater les manquements et infractions aux obligations prévues par :

1° 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 ;

2° 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) nº 526/2013 ;

3° Les chapitres II et III du présent titre ;

4° Les articles L. 100, L. 102 et L. 103 du code des postes et des communications électroniques ;

5° Les exigences de cybersécurité résultant des autorisations, certifications, qualifications et agréments que l'autorité nationale de sécurité des systèmes d'information délivre.

Sous-section 2
**Des pouvoirs**

**Article 27**

La personne faisant l'objet d'un contrôle de l'autorité nationale de sécurité des systèmes d'information met à disposition des agents ou personnes mentionnés à l'article 26, les moyens nécessaires pour effectuer les vérifications sur place et sur pièces et évaluer la conformité aux exigences et le respect des obligations qui lui incombent.

Les agents et personnes mentionnés à l'article 26 ont accès aux locaux des entités contrôlées. Ils peuvent pénétrer dans les lieux à usage professionnel.

En outre, ils peuvent :

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, y compris les éléments de nature à établir la mise en œuvre effective par l'entité des mesures de nature à répondre à ses obligations, dont les rapports d'audit menés par des organismes indépendants ;

2° Recueillir, sur place ou sur demande, tout renseignement ou toute justification utile ;

3° Accéder aux systèmes d'information, aux logiciels, aux programmes informatiques et aux données stockées et en demander la transcription par tout traitement approprié dans des documents directement utilisables pour les besoins de la supervision ;

4° 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.

Le secret professionnel ne peut être opposé par les personnes contrôlées aux personnes mentionnées au premier alinéa agissant dans le cadre des pouvoirs qui leur sont conférés par les dispositions du présent chapitre.

Les agents et les personnes mentionnés à l'article 26 ainsi que les experts qui concourent à l'accomplissement des missions prévues au même article sont astreints au secret professionnel pour les faits, actes ou renseignements dont ils ont connaissance en raison de leurs fonctions, sous réserve des éléments nécessaires à l'établissement des documents d'instruction.

Les rapports, avis ou autres documents justifiant d'adopter les mesures mentionnées aux articles 28, 29 et 32, y compris ceux établis ou recueillis dans le cadre de la recherche de manquement, peuvent être communiqués à la personne faisant l'objet du contrôle.

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

**Article 28**

La personne contrôlée est tenue de coopérer avec l'autorité nationale de sécurité des systèmes d'information. Les agents et les personnes mentionnés à l'article 26 peuvent constater toute action de sa part de nature à faire obstacle au contrôle.

Le fait, pour la personne contrôlée, de faire obstacle aux demandes de l'autorité nationale de sécurité des systèmes d'information nécessaires à la recherche des manquements et à la mise en œuvre des pouvoirs prévus par la présente sous-section, notamment en fournissant des renseignements incomplets ou inexacts ou en communiquant des pièces incomplètes ou dénaturées, est constitutif d'un manquement et puni d'une amende administrative prononcée par la commission des sanctions mentionnée à l'article 35 dont le montant, proportionné à la gravité du manquement, ne peut excéder dix millions d'euros ou 2 % du chiffre d'affaires annuel mondial, hors taxes, de l'exercice précédent, le montant le plus élevé étant retenu.

L'autorité nationale de sécurité des systèmes d'information notifie à la personne contrôlée les griefs constitutifs d'obstacle mentionné à l'alinéa précédent retenus à son encontre, et saisit la commission des sanctions mentionnée à l'article 35 qui se prononce dans les conditions prévues à la section 3 du présent chapitre.

Les dispositions du présent article ne s'appliquent pas aux administrations de l'Etat et à ses établissements publics administratifs.

**Article 29**

Le contrôle de l'autorité nationale de sécurité des systèmes d'information peut prendre la forme suivante :

1° Inspections sur place et contrôles à distance ;

2° Audits de sécurité réguliers et ciblés réalisés par l'autorité nationale mentionnée au premier alinéa ou par un organisme indépendant choisi par cette dernière ;

3° Scans de sécurité ;

4° Audits en cas d'incident important ou d'une violation des dispositions de l'article 26.

Le coût de ces mesures est à la charge des personnes contrôlées sauf lorsque, à titre exceptionnel, l'autorité nationale de sécurité des systèmes d'information en décide autrement.

**Article 30**

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

Section 2
**Mesures consécutives aux contrôles**

**Article 31**

Au vu des résultats du contrôle réalisé en application des dispositions de la section 1, l'autorité nationale de sécurité des systèmes d'information peut décider de l'ouverture d'une procédure à l'encontre de la personne contrôlée. Elle lui notifie sa décision.

L'autorité nationale de sécurité des systèmes d'information désigne parmi les agents et personnes mentionnés à l'article 26 un ou plusieurs rapporteurs chargés de l'instruction de cette procédure.

**Article 32**

Lorsque cette instruction ne fait pas état de faits justifiant une mesure d'exécution, l'autorité nationale de sécurité des systèmes d'information clôt la procédure et en informe la personne concernée.

Dans le cas contraire, l'autorité nationale peut, après avoir mis la personne concernée en mesure de présenter ses observations :

1° Prononcer une mise en garde à son encontre ;

2° Lui enjoindre de prendre les mesures nécessaires pour éviter un incident ou y remédier, et définir les délais pour mettre en œuvre ces mesures et rendre compte de cette mise en œuvre ;

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

4° Lui ordonner d'informer les personnes physiques ou morales à l'égard desquelles elle fournit des services ou exerce des activités susceptibles d'être affectées par une cybermenace importante, de la nature de cette menace, ainsi que de toutes mesures préventives ou réparatrices que ces personnes physiques ou morales pourraient prendre en réponse à cette menace ;

5° Lui enjoindre de mettre en œuvre dans le délai qu'elle fixe les recommandations formulées à la suite d'un audit de sécurité ;

6° Exiger qu'elle communique au public le manquement constaté par tout moyen adapté.

La mesure d'exécution est notifiée aux intéressés et assortie, le cas échéant, d'une astreinte dont le montant ne peut excéder 5 000 euros par jour de retard. L'autorité nationale de la sécurité des systèmes d'information peut décider de la rendre publique.

L'astreinte journalière court à compter du jour suivant l'expiration du délai imparti aux personnes concernées pour déférer à l'injonction. En cas d'inexécution totale ou partielle ou d'exécution tardive, la commission des sanctions mentionnée à l'article 35 peut procéder à la liquidation de l'astreinte.

**Article 33**

Lorsque la personne concernée apporte les éléments montrant qu'elle s'est conformée à la mesure d'exécution mentionnée à l'article 32 dans le délai imparti, l'autorité nationale de sécurité des systèmes d'information constate qu'il n'y a pas lieu de poursuivre la procédure et le notifie à cette personne.

Lorsque la personne en cause ne se conforme pas à l'une des mesures d'exécution qui lui est adressée, l'autorité nationale de sécurité des systèmes d'information lui notifie les griefs et saisit la commission des sanctions mentionnée à l'article 35.

Lorsque la personne concernée est une entité essentielle et qu'elle n'apporte pas la preuve qu'elle s'est conformée aux mesures d'exécution mentionnées aux 1° à 3° et 5° de l'article 32 dans le délai imparti, l'autorité nationale de sécurité des systèmes d'information peut suspendre une certification ou une autorisation concernant tout ou partie des services fournis ou des activités exercées par l'entité jusqu'à ce que l'entité essentielle ait remédié au manquement. Lorsque cette certification ou cette autorisation a été délivrée par à un organisme de certification ou d'autorisation par un autre organisme, elle enjoint à cet organisme de la suspendre jusqu'à ce que l'entité essentielle ait remédié au manquement.

**Article 34**

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

Section 3
**Des sanctions**

**Article 35**

La commission des sanctions mentionnée à l'article L. 1332-15 du code de la défense statue sur les manquements constatés aux obligations découlant de l'application des chapitres II et III du présent titre, dans les conditions prévues par la présente section.

**Article 36**

Lorsqu'elle est saisie de manquements aux obligations découlant de l'application des chapitres II et III du présent titre, la commission des sanctions est composée :

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

2° De trois personnalités qualifiées, nommées par le Premier ministre en raison de leurs compétences dans le domaine de la sécurité des systèmes d'information.

**Article 37**

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

1° A l'encontre des entités essentielles et des opérateurs mentionnés à l'article L. 1332-2 du code de la défense, à l'exception des administrations de l'Etat et de ses établissements publics administratifs, des collectivités territoriales, de leurs groupements et de leurs établissements publics administratifs, une amende administrative dont le montant, proportionné à la gravité du manquement, ne peut excéder 10 millions d'euros ou 2 % du chiffre d'affaires annuel mondial, hors taxes, de l'exercice précédent de l'entreprise à laquelle l'entité essentielle appartient, le montant le plus élevé étant retenu ;

2° A l'encontre des entités importantes, à l'exception des administrations de l'Etat et de ses établissements publics administratifs, des collectivités territoriales, de leurs groupements et de leurs établissements publics administratifs, une amende administrative dont le montant, proportionné à la gravité du manquement, ne peut excéder 7 millions d'euros ou 1,4 % du chiffre d'affaires annuel mondial total, hors taxes, de l'exercice précédent de l'entreprise à laquelle l'entité importante appartient, le montant le plus élevé étant retenu ;

3° A l'encontre des offices d'enregistrement et des bureaux d'enregistrement mentionnés à l'article 18 de la présente loi, à l'exception de ceux relevant des articles L. 45 à L. 45-8 du code des postes et des communications électroniques lorsqu'il s'agit d'un manquement aux obligations prévues à la section 3 du chapitre II de la présente loi, une amende administrative dont le montant, proportionné à la gravité du manquement, ne peut excéder 7 millions d'euros ou 1,4 % du chiffre d'affaires annuel mondial total, hors taxes, de l'exercice précédent. Cette amende peut se cumuler avec l'amende prévue au 1° prononcée à l'encontre d'un office d'enregistrement en cas de manquement aux obligations applicables aux entités essentielles.

Si les manquements relevés constituent également une violation du règlement (UE) n° 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE, donnant lieu à un amende administrative prononcée par la Commission nationale de l'informatique et des libertés en vertu des articles 20 à 22-1 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, la commission des sanctions ne peut prononcer de sanction sous forme d'amende administrative.

II. – La commission des sanctions peut prononcer une amende administrative dont le montant, proportionné à la gravité du manquement, ne peut excéder 10 millions d'euros ou 2 % du chiffre d'affaires annuel mondial total, hors taxes, de l'exercice précédent, le montant le plus élevé étant retenu, à l'encontre :

1° Des fournisseurs de moyens d'identification électronique relevant des schémas d'identification électronique notifiés par l'Etat, des prestataires de services de confiance établis sur le territoire français, des fournisseurs de dispositifs de création de signature et de cachet électronique qualifié qu'elle certifie et des organismes d'évaluation de la conformité, à l'exception des administrations de l'Etat et de leurs établissements publics à caractère administratif, en cas de manquement constaté aux dispositions du règlement (UE) n° 910/2014 du 23 juillet 2014 mentionné ci-dessus ;

2° Des organismes d'évaluation de la conformité sauf si l'organisme d'évaluation de la conformité est l'autorité nationale de certification de cybersécurité, des titulaires d'une déclaration de conformité aux exigences d'un schéma de certification européen, des titulaires d'un agrément, d'une qualification ou d'un certificat dans le domaine de la cybersécurité, en cas de manquement constaté aux dispositions du règlement (UE) n° 2019/881 du 17 avril 2019 mentionné ci-dessus ou aux exigences applicables mentionnés au 4° et au 5° de l'article 26 de la présente loi.

III. – Lorsque la commission des sanctions envisage également de prononcer l'amende prévue à l'article 28 à l'encontre de la même personne, le montant cumulé des sanctions ne peut excéder le montant maximum de l'amende prévue au I ou au II du présent article.

IV. – La commission des sanctions peut également prononcer les mesures suivantes à l'encontre des organismes d'évaluation de la conformité et des titulaires d'agréments, de qualifications ou de certificats en matière de cybersécurité, au titre des dispositions du règlement (UE) n° 910/2014 du 23 juillet 2014 mentionné ci-dessus, des dispositions du règlement (UE) 2019/881 du 17 avril 2019 mentionné ci-dessus ou des exigences de cybersécurité mentionnés au 5° de l'article 26 de la présente loi :

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

2° L'abrogation de l'autorisation, de l'agrément ou de l'habilitation délivré à l'organisme d'évaluation de la conformité, lorsque le manquement n'est pas corrigé dans le délai imparti par l'autorité nationale de sécurité des systèmes d'information.

V. – La commission des sanctions peut interdire à toute personne physique exerçant les fonctions de dirigeant dans l'entité essentielle d'exercer des responsabilités dirigeantes dans cette entité, jusqu'à ce que l'entité essentielle ait remédié au manquement. Ces dispositions ne s'appliquent pas aux administrations.

## CHAPITRE IV
## DISPOSITIONS DIVERSES D'ADAPTATION

### Article 38

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

1° L'article 30 est remplacé par les dispositions suivantes :

« *Art. 30.* – I. – L'utilisation des moyens de cryptologie est libre.

« II. – La fourniture, le transfert depuis ou vers un Etat membre de l'Union européenne, l'importation et l'exportation des moyens de cryptologie assurant exclusivement des fonctions d'authentification ou de contrôle d'intégrité sont libres.

« III. – La fourniture, le transfert depuis ou vers un Etat membre de l'Union européenne, l'importation et l'exportation d'un moyen de cryptologie n'assurant pas exclusivement des fonctions d'authentification ou de contrôle d'intégrité sont soumis à une déclaration préalable auprès du Premier ministre, sauf dans les cas prévus au *b* du présent III et sans préjudice des exigences applicables aux biens à double usage intégrant un moyen de cryptologie. Un décret en Conseil d'Etat fixe :

« *a*) 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 ;

« *b*) Les catégories de moyens dont les caractéristiques techniques ou les conditions d'utilisation sont telles que, au regard des intérêts de la défense nationale et de la sécurité intérieure ou extérieure de l'Etat, leur fourniture, leur transfert depuis ou vers un Etat membre de l'Union européenne ou leur importation ou exportation peuvent être dispensés de toute formalité préalable. » ;

2° L'article 33 est abrogé ;

3° Le I de l'article 35 est remplacé par les dispositions suivantes :

« 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 Etat 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**

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

1° A l'article L. 2321-2-1 :

*a)* Au premier alinéa, 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 de la loi n° ….. du ….. relative à la résilience des infrastructures critiques et au renforcement de la cybersécurité » ;

*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 de la loi n° ….. du ….. mentionnée ci-dessus » ;

2° A l'article L. 2321-3 :

*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 de la loi n° ….. du ….. relative à la résilience des infrastructures critiques et au renforcement de la cybersécurité » ;

*b)* Au deuxième alinéa, les mots : « 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 de la loi n° ….. du ….. mentionnée ci-dessus ».

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

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

*a)* Au *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 ;

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

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

*c)* A l'avant-dernier alinéa du I, les mots : « *n ter* et *o* du présent I » sont remplacés par les mots : « *n ter*, *o* et *r* du présent I » ;

*d)* Après le 3° du VII, il est inséré un 4° ainsi rédigé :

« 4° Les dispositions du *r* du I sont applicables en Polynésie française, dans les îles Wallis et Futuna et en Nouvelle-Calédonie. » ;

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

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

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

4° A l'article 45-4 :

*a)* La première phrase du premier alinéa est complétée par les mots : « ainsi que par les agents agissant pour le compte de ces derniers » ;

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

*c)* Le dernier alinéa est complété avec 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. » ;

*d)* Il est ajouté un alinéa ainsi rédigé :

« Le décret en Conseil d'Etat prévu à l'article L. 45-7 précise les catégories d'agents pouvant agir pour le compte des bureaux d'enregistrement. » ;

5° A l'article L. 45-5 :

*a)* Le deuxième alinéa est remplacé par les dispositions suivantes :

« Les offices d'enregistrement, par l'intermédiaire des bureaux d'enregistrement ainsi que des agents agissant pour le compte de ces derniers, collectent les données nécessaires à l'enregistrement des noms de domaine, notamment celles relatives à l'identification des personnes physiques ou morales titulaires de ces noms de domaine et des personnes chargées de leur gestion. Après leur enregistrement, et sans retard injustifié, les offices et les bureaux d'enregistrement rendent publiques, au moins quotidiennement, ces données dès lors qu'elles n'ont pas de caractère personnel. Ils tiennent ces bases de données à jour, en maintenant les données exactes et complètes, sans redondance de collecte, et sont responsables du traitement de ces données dans le respect de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. » ;

*b)* Au dernier alinéa, après le mot : « inexactes » sont insérés les mots : « ou incomplètes » ;

*c)* Sont ajoutés deux alinéas ainsi rédigés :

« Les offices et les bureaux d'enregistrement répondent aux demandes d'accès aux données d'enregistrement dans un délai n'excédant pas soixante-douze heures après réception de la demande.

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

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

III. – 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.

IV. – 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 :

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

2° Les articles 9 et 12 sont abrogés ;

3° Le I de l'article 14 est abrogé.

**Article 40**

I. – Le titre II de la présente loi, à l'exception de son article 13, est applicable dans les îles Wallis et Futuna, en Polynésie française, en Nouvelle-Calédonie et dans les Terres australes et antarctiques françaises, sous réserve des adaptations suivantes :

1° En l'absence d'adaptation, les références faites, par des dispositions du titre II applicables en Polynésie française et en Nouvelle-Calédonie, à des dispositions qui n'y sont pas applicables sont remplacées par les références aux dispositions ayant le même objet applicables localement ;

2° Dans les îles Wallis et Futuna, en Polynésie française et en Nouvelle-Calédonie, les sanctions pécuniaires encourues en vertu du titre II de la présente loi sont prononcées en monnaie locale, compte tenu de la contre-valeur de l'euro dans cette monnaie.

II. – L'article 13 de la présente loi n'est pas applicable à Saint-Barthélemy et à Saint-Pierre-et-Miquelon.

III. – Pour l'application du titre II à Saint-Barthélemy, Saint-Pierre-et-Miquelon, dans les îles Wallis et Futuna, en Polynésie française, en Nouvelle-Calédonie et dans les Terres australes et antarctiques françaises, les références à la directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, au règlement (UE) n° 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE, au règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive n° 1999/93/CE et au 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 sont remplacées par la référence aux règles en vigueur en métropole en vertu de la même directive et des mêmes règlements.

IV. – Le I de l'article 57 de la loi n° 2004-575 du 21 juin 2004 mentionnée ci-dessus est ainsi modifié :

1° Au premier alinéa, les mots : « articles 1er à 8, 14 à 20, 25 et 29 à 49 » sont remplacés par les mots : « articles 1er à 8, 14 à 20, 25, 29, 30, 31 et 37 à 49 » et les mots : « loi n° 2022-1159 du 16 août 2022 portant diverses dispositions d'adaptation au droit de l'Union européenne en matière de prévention de la diffusion de contenus à caractère terroriste en ligne » sont remplacés par les mots : « loi n° ….. du ….. relative à la résilience des infrastructures critiques et au renforcement de la cybersécurité » ;

2° Au deuxième alinéa, les mots : « articles 8, 14, 19, 25 et 29 à 49 » sont remplacés par les mots : « articles 8, 14, 19, 25, 29, 30, 31 et 37 à 49 » et après les mots : « Terres australes et antarctiques françaises » sont insérés les mots « dans leur rédaction résultant de la loi n° ….. du ….. relative à la résilience des infrastructures critiques et au renforcement de la cybersécurité » ;

3° Au troisième alinéa, les mots : « articles 35 à 38 et 41 à 49, qui s'appliquent de plein droit dans cette collectivité, les articles 1er à 8, 14 à 20, 25, 29 à 34, 39 et 40 » sont remplacés par les mots : « articles 37, 38 et 41 à 49, qui s'appliquent de plein droit dans cette collectivité, les articles 1er à 8, 14 à 20, 25, 29, 30, 31, 37, 39 et 40 ».

V. – 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 remplacé par les dispositions suivantes :

« 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. »

VI. – L'article 16 de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives, après les mots : « dans les îles Wallis et Futuna » 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 ELECTRONIQUES

### Article 41

L'article L. 39-1 du code des postes et des communications électroniques est remplacé par les dispositions suivantes :

« *Art. L. 39-1.* – I. – Est puni de six mois d'emprisonnement et de 30 000 euros d'amende le fait :

« 1° De maintenir un réseau indépendant en violation d'une décision de suspension ou de retrait du droit d'établir un tel réseau ;

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

« *a*) Dans des conditions non conformes aux dispositions de l'article L. 34-9 ;

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

« *c*) En dehors des conditions de ladite autorisation lorsque celle-ci est requise ;

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

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

« *f*) Sans l'accord ou l'avis mentionné au I de l'article L. 43 ou en dehors des caractéristiques déclarées lors de la demande de cet accord ou de cet avis.

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

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

« *a*) Dans des conditions non conformes aux dispositions de l'article L. 34-9 ;

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

« *c*) En dehors des conditions de ladite autorisation lorsque celle-ci est requise ;

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

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

« *f*) Sans l'accord ou l'avis mentionné au I de l'article L. 43 ou en dehors des caractéristiques déclarées lors de la demande de cet accord ou de cet avis ;

« 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.

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

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

« 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 des dispositions 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

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

1° Au I :

*a)* Le 1. est remplacé par les dispositions suivantes :

« 1. Toute demande d'assignation de fréquence relative à un système satellitaire est adressée à l'Agence nationale des fréquences.

« 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.

« Cette déclaration est effectuée sous réserve :

« – de la conformité de l'assignation demandée avec le tableau national de répartition des bandes de fréquences et aux stipulations des instruments de l'Union internationale des télécommunications ;

« – 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 ;

« – que les assignations soumises ne soient pas de nature à compromettre les intérêts de la sécurité nationale et le respect par la France de ses engagements internationaux. » ;

*b)* Au 2. :

*i)* Après le deuxième alinéa, il est inséré un alinéa ainsi rédigé :

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

*ii)* Au 1°, après le mot : « défense », il est inséré le mot : « nationale » et après les mots : « sécurité publique » sont ajoutés les mots : « ainsi que le respect par la France de ses engagements internationaux » ;

*iii)* Après le 4°, sont insérés un 5° et un 6° ainsi rédigés :

« 5° Lorsque le demandeur ne peut démontrer qu'un intérêt économique s'attache, pour la France, à l'autorisation ;

« 6° Lorsque le demandeur est dans l'incapacité technique ou financière de faire face durablement aux obligations qui sont les siennes une fois l'autorisation obtenue. » ;

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

« Elle peut être assortie, le cas échéant, de conditions visant à assurer que les activités prévues dans le cadre de l'exploitation de l'assignation autorisée ne porteront pas atteinte aux intérêts de la sécurité et de la défense nationale ou au respect par la France de ses engagements internationaux. » ;

2° Le second alinéa du III est remplacé par les dispositions suivantes :

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

« Après que l'intéressé a reçu la notification des 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.

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

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

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

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

« – l'interruption de la procédure engagée par la France auprès de l'Union internationale des télécommunications.

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

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

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

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

3° Le VI est remplacé par les dispositions suivantes :

« VI. – Un décret en Conseil d'Etat fixe les modalités d'application du présent article. Il précise :

« 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 ;

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

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

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

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

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

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

II. – A l'article L. 97-4 du même code, après les mots : « les articles L. 97-2 » sont insérés les mots : « , dans sa rédaction résultant de la loi n° ….. du ….. , ».

III. – Les dispositions du présent article s'appliquent à compter de l'entrée en vigueur du décret prévu au VI et au plus tard le 31 décembre 2025.

## TITRE III
## RESILIENCE OPERATIONNELLE NUMERIQUE DU SECTEUR FINANCIER

### CHAPITRE Ier
### DISPOSITIONS MODIFIANT LE CODE MONETAIRE ET FINANCIER

### Article 43

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

L'article L. 420-3 du même code est ainsi modifié :

1° Au I :

*a)* A 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 fixées 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) n° 2016/1011 pour garantir » et le mot : « tension » est remplacé par les mots : « graves tensions » ;

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

*c)* A la troisième phrase, après les mots : « continuité des 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 mis en place conformément à l'article 11 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) n° 2016/1011 afin d'assurer le maintien de ses services » ;

2° Au III :

*a)* Au premier alinéa, après les mots : « environnements de tests » sont insérés les mots : « conformément aux exigences fixées aux chapitres II et IV du règlement (UE) n° 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) n° 2016/1011 » et les mots : « s'assurer » sont remplacés par le mot : « garantir » ;

*b)* Au deuxième alinéa, après les mots : « forme de négociation, », il est inséré le mot : « afin ».

**Article 45**

I. – A l'article L. 421-4 du même code, les mots : « aux alinéas 2 et 4 » sont remplacés par les mots : « au 2. ».

II. – L'article L. 421-11 du même code est ainsi modifié :

1° Au I :

*a)* Au 2., après les mots : « suivi adéquats 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) n° 2016/1011, et » ;

*b)* Le 4. est abrogé ;

2° A la seconde phrase du premier alinéa du III, les mots : « aux 2 et 4 » sont remplacés par les mots : « au 2. » ;

3° A la seconde phrase du second alinéa, les mots : « aux 2 et 4 » sont remplacés par les mots : « au 2. ».

**Article 46**

L'article L. 511-41-1-B du même code est ainsi modifié :

1° Au deuxième alinéa :

*a)* Après les mots : « le risque 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) n° 2016/1011 y compris ceux liés aux services de technologies de l'information et de la communication fournis par les prestataires tiers » ;

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

2° Au cinquième alinéa :

*a)* Après les mots : « risques encourus, établir » sont insérés les mots : « des politiques et » ;

*b)* Après les mots : « de leur 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**

Au premier alinéa de l’article L. 511-55 du même code, après les mots : « et comptables saines, » sont insérés les mots : « de réseaux et de systèmes d’information qui sont 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) n° 2016/1011, ».

**Article 48**

L'article L. 521-9 du même code est complété par un alinéa ainsi rédigé :

« Ils se conforment en outre aux exigences du chapitre II du règlement (UE) n° 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) n° 2016/1011 applicables aux prestataires de services de paiement visés au I de l'article L. 521-1. »

**Article 49**

L’article L. 521-10 du même code est ainsi modifié :

1° Au I, après les mots : « services de paiement » sont insérés les mots : « mentionnés au II de l’article L. 521-1 » ;

2° A la première phrase du II, le mot : « informent » est remplacé par les mots : « mentionnés au II de l’article L. 521-1 informent » ;

3° Au III, après la deuxième occurrence des mots : « services de paiement » sont insérés les mots : « mentionné au II de l’article L. 521-1 ».

**Article 50**

Au premier alinéa de l’article L. 533-2 du même code, après les mots : « leurs systèmes informatiques » sont insérés les mots : « , y compris les réseaux et les systèmes d’information qui sont mis en place et gérés conformément au règlement (UE) n° 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) n° 2016/1011 ».

**Article 51**

L’article L. 533-10 du même code est ainsi modifié :

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

« 6° A l'exception de celles 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, mettent en place des procédures administratives et comptables saines, des dispositifs de contrôle et de sauvegarde dans le domaine du traitement électronique des données, y compris les réseaux et les systèmes d'information qui sont mis en place et gérés conformément au règlement (UE) n° 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) n° 2016/1011. » ;

2° Au II :

*a)* A la première phrase du 4°, après les mots : « utilisant des 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) n° 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) n° 2016/1011 » ;

*b)* Au 5° :

– après les mots : « solides pour garantir » sont insérés les mots : « , conformément aux exigences fixées 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) n° 2016/1011, » ;

– après les mots : « de l'information, », il est inséré le mot : « pour » ;

– après les mots : « non autorisé et », il est inséré le mot : « pour ».

**Article 52**

L'article L. 533-10-4 du même code est ainsi modifié :

1° Au *a* du 1°, après les mots : « une capacité suffisante » sont insérés les mots : « , conformément aux exigences fixées au chapitre II du règlement (UE) n° 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) n° 2016/1011 » ;

2° Au 2° :

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

*b)* Après les mots : « systèmes de 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 conformément à l'article 11 du règlement (UE) n° 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 précité » ;

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

**Article 53**

Au troisième alinéa de l'article L. 612-24 du même code, après les mots : « ou activités opérationnelles » sont insérés les mots : « y compris les prestataires tiers, en particulier critiques, de services fondés sur les technologies de l'information et de la communication visés au chapitre V du règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) n° 1060/2009, (UE) n° 648/2012, (UE) n° 600/2014, (UE) n° 909/2014 et (UE) n° 2016/1011, ».

**Article 54**

Le III de l'article L. 613-38 du même code est ainsi modifié :

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

2° Le 17° est complété par les mots : « , y compris des réseaux et des systèmes d'information visés dans le règlement (UE) n° 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) n° 2016/1011 ».

**Article 55**

Le quatrième alinéa du II de l'article L. 631-1 du même code est remplacé par les dispositions suivantes :

« L'Autorité des marchés financiers, la Banque de France, l'Autorité de contrôle prudentiel et de résolution et l'autorité nationale en charge de la 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 afin d'assurer, en particulier, le respect de la loi n° ….. du ….. et du règlement (UE) n° 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) n° 2016/1011. »

**Article 56**

Le même code est ainsi modifié :

1° Le I de l'article L. 712-7 est complété par un 14° ainsi rédigé :

« 14° 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. » ;

2° Dans le tableau figurant au I des articles L. 752-10, L. 753-10 et L. 754-8, la ligne :

«

| | |
|---|---|
| L. 314-1 | l'ordonnance n° 2017-1433 du 4 octobre 2017 |

»

est remplacée par la ligne suivante :

«

| | |
|---|---|
| L. 314-1 | la loi n° ….. du ….. |

» ;

3° A l'article L. 761-1, les mots : « juillet 2014 et 2022/858 du 30 mai 2022 » sont remplacés par les mots : « juillet 2014, 2022/858 du 30 mai 2022 et 2022/2554 du 14 décembre 2022 » ;

4° Dans le tableau figurant au I des articles L. 762-3, L. 763-3 et L. 764-3, la ligne :

«

| | |
|---|---|
| L. 420-3 à L. 420-5 | l'ordonnance n° 2017-1107 du 22 juin 2017 |

»

est remplacée par les deux lignes suivantes :

«

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

» ;

5° Dans le tableau figurant au I des articles L. 762-4, L. 763-4 et L. 764-4 :

*a)* La ligne :

«

| | |
|---|---|
| L. 421-1 à L. 421-7-2 | l'ordonnance n° 2016-827 du 23 juin 2016 |

»

est remplacée par les trois lignes suivantes :

«

| | |
|---|---|
| L. 421-1 à 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 |

» ;

*b)* La ligne :

«

| | |
|---|---|
| L. 421-11 | l'ordonnance n° 2017-1107 du 22 juin 2017 |

»

est remplacée par la ligne suivante :

«

| | |
|---|---|
| L. 421-11 | la loi n° ….. du ….. |

» ;

6° Aux articles L. 771-1 et L. 781-1, les mots : « décembre 2020 et 2022/858 du 30 mai 2022 » sont remplacés par les mots : décembre 2020, 2022/858 du 30 mai 2022 et 2022/2554 du 14 décembre 2022 » ;

7° Dans le tableau figurant au I des articles L. 773-5, L. 774-5 et L. 775-5, la ligne :

«

| | |
|---|---|
| L. 511-41-1 B et L. 511 41-1 C | l'ordonnance n° 2020-1635 du 21 décembre 2020 |

»

est remplacée par les deux lignes suivantes :

«

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

» ;

8° Dans le tableau figurant au I des articles L. 773-6, L. 774-6 et L. 775-6, la ligne :

«

| | |
|---|---|
| L. 511-55 | l'ordonnance n° 2015-1024 du 20 août 2015 |

»

est remplacée par la ligne suivante :

«

| | |
|---|---|
| L. 511-55 | la loi n° ….. du ….. |

» ;

9° Dans le tableau figurant au I des articles L. 773-21, L. 774-21 et L. 775-15, la ligne :

«

| | |
|---|---|
| L. 521-8 à L. 521-10 | l'ordonnance n° 2017-1252 du 9 août 2017 |

»

est remplacée par les deux lignes suivantes :

«

| | |
|---|---|
| L. 521-8 | l'ordonnance n° 2017-1252 du 9 août 2017 |
| L. 521-9 et L. 521-10 | la loi n° ….. du ….. |

» ;

10° Dans le tableau figurant au I du tableau des articles L. 773-30, L. 774-30 et L. 775-24 :

*a)* La ligne :

«

| | |
|---|---|
| L. 533-2 | l'ordonnance n° 2017-1107 du 22 juin 2017 |

»

est remplacée par la ligne suivante :

«

| | |
|---|---|
| L. 533-2 | la loi n° ….. du ….. |

» ;

*b)* La ligne :

«

| | |
|---|---|
| L. 533-10 | l'ordonnance n° 2021-796 du 23 juin 2021 |

»

est remplacée par la ligne suivante :

«

| | |
|---|---|
| L. 533-10 | la loi n° ….. du ….. |

» ;

*c)* La ligne :

«

| | |
|---|---|
| L. 533-10-2 à L. 533-10-8 | l'ordonnance n° 2016-827 du 23 juin 2016 |

»

est remplacée par les trois lignes suivantes :

«

| | |
|---|---|
| L. 533-10-2 et L. 533-10-3 | 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 |

» ;

11° Dans le tableau figurant au I des articles L. 783-2, L. 784-2 et L. 785-2, la ligne :

«

| | |
|---|---|
| L. 612-24, à l'exception de son huitième alinéa | l'ordonnance n° 2021-796 du 23 juin 2021 |

»

est remplacée par la ligne suivante :

«

| | |
|---|---|
| L. 612-24, à l'exception de son huitième alinéa | la loi n° ….. du ….. |

» ;

12° Dans le tableau figurant au I des articles L. 783-4, L. 784-4 et L. 785-4, la ligne :

«

| | |
|---|---|
| L. 613-38 | l'ordonnance n° 2020-1636 du 21 décembre 2020 |

»

est remplacée par la ligne suivante :

«

| | |
|---|---|
| L. 613-38 | la loi n° ….. du ….. |

» ;

13° Dans le tableau figurant au I des articles L. 783-13, L. 784-13 et L. 785-12, la ligne :

«

| | |
|---|---|
| L. 631-1 | l'ordonnance n° 2020-115 du 12 février 2020 |

»

est remplacée par la ligne suivante :

«

| | |
|---|---|
| L. 631-1 | la loi n° ….. du ….. |

».

## CHAPITRE II
## DISPOSITIONS MODIFIANT LE CODE DES ASSURANCES

### Article 57

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

1° A la première phrase du troisième alinéa, les mots : « à l'article L. 310-3 » sont remplacés par les mots : « au 13° de l'article L. 310-3 » ;

2° La seconde phrase du quatrième alinéa est complétée par les mots : « et, en particulier, mettent en place et gèrent des réseaux et des systèmes d'information conformément au règlement (UE) n° 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) n° 2016/1011 ».

### Article 58

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

1° A la première phrase du troisième alinéa, les mots : « à l'article L. 310-3 » sont remplacés par les mots : « au 13° de l'article L. 310-3 » ;

2° La seconde phrase du quatrième alinéa est complétée par les mots : « et, en particulier, mettent en place et gèrent des réseaux et des systèmes d'information conformément au règlement (UE) n° 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) n° 2016/1011 ».

## CHAPITRE III
## DISPOSITIONS MODIFIANT LE CODE DE LA MUTUALITE

### Article 59

La seconde phrase du quatrième alinéa de l'article L. 211-12 du code de la mutualité est complétée par les mots : « et, en particulier, mettent en place et gèrent des réseaux et des systèmes d'information conformément au règlement (UE) n° 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) n° 2016/1011 ».

### Article 60

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

## CHAPITRE IV
## DISPOSITIONS MODIFIANT LE CODE DE LA SECURITE SOCIALE

### Article 61

La seconde phrase du quatrième alinéa de l'article L. 931-7 du code de la sécurité sociale est complétée par les mots : « et, en particulier, mettent en place et gèrent des réseaux et des systèmes d'information conformément au règlement (UE) n° 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) n° 2016/1011 ».

## CHAPITRE V
## DISPOSITIONS FINALES

### Article 62

Les dispositions du présent titre sont applicables à compter du 17 janvier 2025. Toutefois, les dispositions des articles 46, 47 et 54 sont applicables aux sociétés de financement remplissant les conditions prévues au point 145 du paragraphe 1 de l'article 4 du règlement (UE) n° 575/2013 du Parlement européen et du Conseil du 26 juin 2013 concernant les exigences prudentielles applicables aux établissements de crédit et aux entreprises d'investissement et modifiant le règlement (UE) n° 648/2012 à compter du 17 janvier 2026.