PJL "résilience des infrastructures critiques"

Directives NIS2 + REC : projet de transposition FRANCE

version du 12 mars 2025 adoptée par le Sénat

- document de travail -

**Destinataire** : public professionnel

**Diffusion et utilisation** : libres après téléchargement

Une image contenant texte, habits, Visage humain, capture d’écran

Description générée automatiquement

sommaire

[#PJL#Résilience#article#01# 4](#_Toc201673027)

[1 L.1332-1 Code de la défense [ré-écrit] [modifié Sénat] [OIV AIV PIV] 4](#_Toc201673028)

[2 L.1332-2 Code de la défense [ré-écrit] [OIV désignation] 4](#_Toc201673029)

[3 L.1332-3 Code de la défense [ré-écrit] [OIV analyse des risques] 5](#_Toc201673030)

[4 L.1332-4 Code de la défense [ré-écrit] [OIV analyse des dépendances] 6](#_Toc201673031)

[5 L.1332-5 Code de la défense [ré-écrit] [modifié Sénat] [OIV plan particulier de résilience] 6](#_Toc201673032)

[6 L.1332-6 Code de la défense [ré-écrit] [PIV autorisation d’accès] 7](#_Toc201673033)

[7 L.1332-7 Code de la défense [ré-écrit] [OIV incident de sécurité] 8](#_Toc201673034)

[8 L.1332-8 Code de la défense [nouveau] [entités critiques d’importance européenne particulière] 8](#_Toc201673035)

[9 L.1332-9 Code de la défense [nouveau] [entités critiques d’importance européenne particulière] 8](#_Toc201673036)

[10 L.1332-10 Code de la défense [nouveau] [captation, enregistrement et transmission d’images] 9](#_Toc201673037)

[11 L.1332-11 Code de la défense [nouveau] [OIV obligations] 9](#_Toc201673038)

[12 L.1332-12 Code de la défense [nouveau] [recherche et constatation des manquements] 9](#_Toc201673039)

[13 L.1332-13 Code de la défense [nouveau] [recherche et constatation des manquements] 9](#_Toc201673040)

[14 L.1332-14 Code de la défense [nouveau] [coopérer avec l’autorité administrative] 10](#_Toc201673041)

[15 L.1332-15 Code de la défense [nouveau] [commission des sanctions] 10](#_Toc201673042)

[16 L.1332-16 Code de la défense [nouveau] [commission des sanctions] 10](#_Toc201673043)

[17 L.1332-17 Code de la défense [nouveau] [commission des sanctions] 11](#_Toc201673044)

[18 L.1332-18 Code de la défense [nouveau] [commission des sanctions] 11](#_Toc201673045)

[19 L.1332-19 Code de la défense [nouveau] [décret à suivre…] 12](#_Toc201673046)

[20 L.1332-20 Code de la défense [nouveau] [OIV marché publics] 12](#_Toc201673047)

[21 L.1332-21 Code de la défense [nouveau] [OIV contrats de concession] 12](#_Toc201673048)

[22 L.1332-22 Code de la défense [nouveau] [OIV contrats de concession] 12](#_Toc201673049)

[#PJL#Résilience#article#02# 12](#_Toc201673050)

[23 L.1333-1 Code de la défense [modifié] [matières nucléaires] 12](#_Toc201673051)

[24 L.2113-2 Code de la défense [modifié] [OIV ressortissants étrangers] 13](#_Toc201673052)

[25 L.2151-1 Code de la défense [modifié] [service de sécurité nationale] 13](#_Toc201673053)

[26 L.2151-4 Code de la défense [modifié] [service de sécurité nationale] 14](#_Toc201673054)

[27 L2171-6 Code de la défense [modifié] [service de sécurité nationale] 14](#_Toc201673055)

[28 L.2321-2-1 Code de la défense [modifié] [OIV marqueurs techniques] 14](#_Toc201673056)

[29 L.2321-3 Code de la défense [modifié] [opérateurs de communications électroniques] 15](#_Toc201673057)

[30 L.4231-6 Code de la défense [modifié] [personnes soumises à l'obligation de disponibilité] 16](#_Toc201673058)

[31 226-3 Code pénal [modifié] [dispositifs techniques et sanction pénale] 16](#_Toc201673059)

[32 L.33-1 CPCE [modifié] [services de communications électroniques] 16](#_Toc201673060)

[33 L.33-14 CPCE [modifié] [OIV marqueurs techniques] 19](#_Toc201673061)

[34 L.34-11 CPCE [modifié] [connecter les terminaux au réseau radioélectrique mobile] 20](#_Toc201673062)

[35 L.1333-9 CSP [modifié] [activités nucléaires à faible exposition aux rayonnements ionisants] 20](#_Toc201673063)

[36 L.223-2 CSI [modifié] [systèmes de vidéoprotection] 22](#_Toc201673064)

[37 L.223-8 CSI [modifié] [systèmes de vidéoprotection] 23](#_Toc201673065)

[38 15 loi n°2006-961 [modifié] [mesures techniques logicielles] 23](#_Toc201673066)

[#PJL#Résilience#article#03# 24](#_Toc201673067)

[39 L.6221-2 Code de la défense [nouveau] [St-Barthélémy] 24](#_Toc201673068)

[40 L.6222-1 Code de la défense [nouveau] [St-Barthélémy] 24](#_Toc201673069)

[41 L.6242-2 Code de la défense [nouveau] [St-Pierre-et-Miquelon] 24](#_Toc201673070)

[42 L.6312-3 Code de la défense [nouveau] [Wallis-et-Futuna etc.] 24](#_Toc201673071)

[43 711-1 code pénal [ré-écrit] [Wallis-et-Futuna etc.] 24](#_Toc201673072)

[#PJL#Résilience#article#04# [décret pour entrée en vigueur] 24](#_Toc201673073)

[#PJL#Résilience#article#05# [modifié Sénat] [ANSSI] 25](#_Toc201673074)

[#PJL#Résilience#article#05bis# [nouveau Sénat] [stratégie nationale de cybersécurité] 25](#_Toc201673075)

[#PJL#Résilience#article#06# [modifié Sénat] [NIS2 définitions légales] 25](#_Toc201673076)

[#PJL#Résilience#article#07# [ré-écrit Sénat] [NIS2 secteurs [hautement] critiques] 26](#_Toc201673077)

[#PJL#Résilience#article#08 [modifié Sénat] [NIS2 entités essentielles #EE] 27](#_Toc201673078)

[#PJL#Résilience#article#09# [modifié Sénat] [NIS2 entités importantes #EI] 28](#_Toc201673079)

[#PJL#Résilience#article#10# [NIS2 #EE #EI désignation dérogatoire par PM] 29](#_Toc201673080)

[#PJL#Résilience#article#11# [NIS2 #EE #EI territoire national 29](#_Toc201673081)

[#PJL#Résilience#article#12# [modifié Sénat] [NIS2 liste #EE #EI] 30](#_Toc201673082)

[#PJL#Résilience#article#13# [NIS2 et actes sectoriels] 30](#_Toc201673083)

[#PJL#Résilience#article#14# [modifié Sénat] [NIS2 mesures opérationnelles] 30](#_Toc201673084)

[#PJL#Résilience#article#15# [modifié Sénat] [NIS2 référentiel d'exigences] 31](#_Toc201673085)

[#PJL#Résilience#article#16# [OIV liste des SIIV] 32](#_Toc201673086)

[#PJL#Résilience#article#16bis# [nouveau Sénat] [chiffrement et backdoor] 32](#_Toc201673087)

[#PJL#Résilience#article#17# [modifié Sénat] [NIS2 notification des incidents de sécurité] 32](#_Toc201673088)

[#PJL#Résilience#article#18# [offices et bureaux d’enregistrement] 33](#_Toc201673089)

[#PJL#Résilience#article#19# [offices et bureaux d’enregistrement] 34](#_Toc201673090)

[#PJL#Résilience#article#20# [modifié Sénat] [offices et bureaux d’enregistrement] 34](#_Toc201673091)

[#PJL#Résilience#article#21# [offices et bureaux d’enregistrement] 34](#_Toc201673092)

[#PJL#Résilience#article#22# [offices et bureaux d’enregistrement] 34](#_Toc201673093)

[#PJL#Résilience#article#23# [modifié Sénat] [coopération et échange d’informations] 34](#_Toc201673094)

[#PJL#Résilience#article#24# [agrément ANSSI pour prévention et gestion des incidents] 35](#_Toc201673095)

[#PJL#Résilience#article#25# [mesures imposées par l'ANSSI] 35](#_Toc201673096)

[#PJL#Résilience#article#26A# 35](#_Toc201673097)

[44 L.103 CPCE [modifié Sénat] [service de coffre-fort numérique] 35](#_Toc201673098)

[#PJL#Résilience#article#26# [modifié Sénat] [rechercher et constater les manquements] 36](#_Toc201673099)

[#PJL#Résilience#article#27# [modifié Sénat] [contrôle ANSSI] 36](#_Toc201673100)

[#PJL#Résilience#article#28# [contrôle ANSSI et coopération] 37](#_Toc201673101)

[#PJL#Résilience#article#29# [modifié Sénat] [contrôle de l'ANSSI] 37](#_Toc201673102)

[#PJL#Résilience#article#30# [contrôle de l'ANSSI et décret à suivre…] 38](#_Toc201673103)

[#PJL#Résilience#article#31# [procédure de contrôle] 38](#_Toc201673104)

[#PJL#Résilience#article#32# [supprimé Sénat] [procédure de contrôle] 38](#_Toc201673105)

[#PJL#Résilience#article#33# [modifié Sénat] [procédure de contrôle] 39](#_Toc201673106)

[#PJL#Résilience#article#34# [procédure de contrôle : décret à suivre…] 39](#_Toc201673107)

[#PJL#Résilience#article#35# [commission des sanctions] 39](#_Toc201673108)

[#PJL#Résilience#article#36# [modifié Sénat] [commission des sanctions] 40](#_Toc201673109)

[#PJL#Résilience#article#37# [modifié Sénat] [sanctions possibles] 40](#_Toc201673110)

[#PJL#Résilience#article#38# [supprimé Sénat] [cryptologie] 41](#_Toc201673111)

[#PJL#Résilience#article#39# [supprimé Sénat] 42](#_Toc201673112)

[#PJL#Résilience#article#40# [supprimé Sénat] 44](#_Toc201673113)

[#PJL#Résilience#article#41# [supprimé Sénat] 44](#_Toc201673114)

[#PJL#Résilience#article#42# [supprimé Sénat] 45](#_Toc201673115)

NB : code couleur

[ gris ] articles du PJL Résilience

[ jaune ] modifications d'articles existants [Code défense, CPCE, CSI, Code pénal, etc.]

[ bleu ] articles existants entièrement ré-écrits ou franchement nouveaux

[ vert ] modifications / suppression par le Sénat

##### #PJL#Résilience#article#01#

TITRE Ier Résilience des activités d’importance vitale

Chapitre Ier Dispositions générales

CHAPITRE II Code de la défense : ~~Protection des installations d'importance vitale~~ Résilience des activités d’importance vitale

Section 1 Code de la défense - Dispositions générales relatives aux activités d’importance vitale

# L.1332-1 Code de la défense [ré-écrit] [modifié Sénat] [OIV AIV PIV]

~~Les opérateurs publics ou privés exploitant des établissements ou utilisant des installations et ouvrages, dont l'indisponibilité risquerait de diminuer d'une façon importante le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la nation, sont tenus de coopérer à leurs frais dans les conditions définies au présent chapitre, à la protection desdits établissements, installations et ouvrages contre toute menace, notamment à caractère terroriste. Ces établissements, installations ou ouvrages sont désignés par l'autorité administrative.~~

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, sont notamment distingués :

a) Les points d’importance vitale, c’est‑à‑dire les installations les plus sensibles, notamment celles qui sont difficilement substituables ;

b) Les systèmes d’information d’importance vitale, c’est-à-dire les systèmes d’information nécessaires à l’exercice d’une activité d’importance vitale ou à la gestion, à l’utilisation ou à la protection d’une ou plusieurs infrastructures critiques ;

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

4° Résilience : la capacité d’un opérateur à prévenir, à se protéger et à résister contre tout type d’incident afin d’assurer la continuité de la ou des activités d’importance vitale qu’il exerce.

# L.1332-2 Code de la défense [ré-écrit] [OIV désignation]

~~Les obligations prescrites par le présent chapitre peuvent être étendues à des établissements mentionnés à l'article~~ [~~L.511-1~~](https://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000006074220&idArticle=LEGIARTI000006834227&dateTexte=&categorieLien=cid) ~~du code de l'environnement ou comprenant une installation nucléaire de base visée à l'article~~ [~~L.593-1~~](https://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000006074220&idArticle=LEGIARTI000025109676&dateTexte=&categorieLien=cid) ~~du code de l'environnement quand la destruction ou l'avarie de certaines installations de ces établissements peut présenter un danger grave pour la population. Ces établissements sont désignés par l'autorité administrative.~~

I. – Sont désignés opérateurs d’importance vitale par l’autorité administrative :

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

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 [REC] en établissant une liste de services essentiels et qui, à ce titre, justifient que cet opérateur soit regardé comme une entité critique au sens de cette directive ;

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 Code de la défense - Dispositions applicables aux opérateurs d’importance vitale

# L.1332-3 Code de la défense [ré-écrit] [OIV analyse des risques]

~~Les opérateurs dont un ou plusieurs établissements, installations et ouvrages sont désignés en application du présent chapitre réalisent pour chacun d'eux les mesures de protection prévues à un plan particulier de protection dressé par l'opérateur et approuvé par l'autorité administrative.~~

~~Ces mesures comportent notamment des dispositions efficaces de surveillance, d'alarme et de protection matérielle. En cas de non-approbation du plan et de désaccord persistant, la décision est prise par l'autorité administrative.~~

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 est réévaluée au moins tous les quatre ans.

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

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 met en demeure l’opérateur de le réaliser, de le modifier ou de le mettre en œuvre dans un délai qu’elle fixe et qui ne 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 à compter de l’expiration du délai imparti par la mise en demeure.

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 Ier et du chapitre III du titre IX du livre V du code de l’environnement.

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

# L.1332-4 Code de la défense [ré-écrit] [OIV analyse des dépendances]

~~En cas de refus des opérateurs de préparer leur plan particulier de protection, l'autorité administrative met, par arrêtés, les chefs d'établissements ou d'entreprises assujettis en demeure de l'établir dans le délai qu'elle fixe.~~

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 du présent chapitre.

# L.1332-5 Code de la défense [ré-écrit] [modifié Sénat] [OIV plan particulier de résilience]

~~Le plan de protection établi dans les conditions prévues à l'article~~ [~~L.1332-4~~](https://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000006071307&idArticle=LEGIARTI000006539694&dateTexte=&categorieLien=cid)~~, l'autorité administrative met, par arrêtés, les chefs d'établissements ou d'entreprises en demeure de le réaliser dans le délai qu'elle fixe.~~

Les opérateurs pour lesquels 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 met en demeure l’opérateur de le réaliser, de le modifier ou de le mettre en œuvre dans un délai qu’elle fixe et qui ne 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 à compter de l’expiration du délai imparti par la mise en demeure.

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.

# L.1332-6 Code de la défense [ré-écrit] [PIV autorisation d’accès]

~~Les arrêtés de mise en demeure prévus aux articles~~ [~~L.1332-4~~](https://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000006071307&idArticle=LEGIARTI000006539694&dateTexte=&categorieLien=cid) ~~et~~ [~~L.1332-5~~](https://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000006071307&idArticle=LEGIARTI000006539696&dateTexte=&categorieLien=cid) ~~fixent un délai qui ne peut être inférieur à un mois, et qui est déterminé en tenant compte des conditions de fonctionnement de l'opérateur et des travaux à exécuter.~~

~~Les arrêtés concernant les entreprises nationales ou faisant appel au concours financier de l'Etat sont transmis au ministre de tutelle et au ministre de l'économie et des finances, qui sont immédiatement informés des difficultés susceptibles de se produire dans l'application de l'arrêté.~~

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

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 du présent code en tenant compte, le cas échéant, de critères déterminés par l’autorité administrative en fonction du secteur d’activité de l’opérateur.

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

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.

# L.1332-7 Code de la défense [ré-écrit] [OIV incident de sécurité]

~~Est puni d'une amende de 150 000 euros le fait, pour les dirigeants des opérateurs mentionnés à l'article~~ [~~L.1332-4~~](https://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000006071307&idArticle=LEGIARTI000006539694&dateTexte=&categorieLien=cid) ~~et à l'expiration du délai défini par l'arrêté de mise en demeure, d'omettre d'établir un plan de protection ou de réaliser les travaux prévus.~~

~~Est puni d'une amende de 150 000 euros le fait, pour les mêmes personnes, d'omettre, après une mise en demeure, d'entretenir en bon état les dispositifs de protection antérieurement établis.~~

~~Est puni d'une amende de 150 000 € le fait, pour les mêmes personnes, de ne pas satisfaire aux obligations prévues aux~~ [~~articles L.1332-6-1 à L.1332-6-4~~](https://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000006071307&idArticle=LEGIARTI000028342852&dateTexte=&categorieLien=cid)~~. Hormis le cas d'un manquement à~~ [~~l'article L.1332-6-2,~~](https://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000006071307&idArticle=LEGIARTI000028342854&dateTexte=&categorieLien=cid) ~~cette sanction est précédée d'une mise en demeure.~~

~~Les personnes morales déclarées responsables, dans les conditions prévues à~~ [~~l'article 121-2~~](https://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000006070719&idArticle=LEGIARTI000006417202&dateTexte=&categorieLien=cid) ~~du code pénal, des infractions prévues à la présente section encourent une amende suivant les modalités prévues à~~ [~~l'article 131-38~~](https://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000006070719&idArticle=LEGIARTI000006417333&dateTexte=&categorieLien=cid) ~~du même code.~~

Les opérateurs d’importance vitale désignés au titre du 1° du I de l’article L.1332-2 notifient à l’autorité administrative, au plus tard vingt‑quatre heures après en avoir pris connaissance, tout incident susceptible de compromettre la continuité de leurs activités d’importance vitale dans des conditions fixées par décret en Conseil d’État.

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 Code de la défense - Dispositions applicables aux entités critiques d’importance européenne particulière

# L.1332-8 Code de la défense [nouveau] [entités critiques d’importance européenne particulière]

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

Ces opérateurs sont identifiés comme entités critiques d’importance européenne particulière dans les conditions prévues à l’article 17 de la directive [REC].

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’État.

# L.1332-9 Code de la défense [nouveau] [entités critiques d’importance européenne particulière]

Lorsque l’opérateur a été désigné par la Commission européenne comme entité critique d’importance européenne particulière il peut, sur demande motivée de la Commission européenne ou d’un ou de plusieurs des États membres auxquels ou dans lesquels le service essentiel est fourni et avec l’accord de l’autorité administrative compétente, faire l’objet d’une mission de conseil au titre de laquelle il doit garantir l’accès aux informations, systèmes et installations relatifs à la fourniture de ses services essentiels qui sont nécessaires à l’exécution de cette mission de conseil, dans le respect des secrets protégés par la loi.

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.

Sous-section 3 Code de la défense - Dispositifs techniques concourant à la protection des installations d’importance vitale

# L.1332-10 Code de la défense [nouveau] [captation, enregistrement et transmission d’images]

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

Sous‑section 4 Code de la défense - Dispositions applicables aux systèmes d’information

# L.1332-11 Code de la défense [nouveau] [OIV obligations]

I. – Pour gérer les risques qui menacent la sécurité des réseaux et des systèmes d’information qu’ils utilisent dans le cadre de leurs activités ou de la fourniture de leurs services, les opérateurs d’importance vitale mettent en œuvre les obligations prévues aux articles 14 à 16 et au premier alinéa de l’article 17 de la loi [résilience].

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 Code de la défense - Contrôles et sanctions administratives

Sous-section 1 Code de la défense - Habilitation et contrôles

# L.1332-12 Code de la défense [nouveau] [recherche et constatation des manquements]

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

# L.1332-13 Code de la défense [nouveau] [recherche et constatation des manquements]

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’État et des collectivités territoriales ainsi que dans les entreprises ou services concédés par l’État, 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. À ce titre, ils peuvent exiger la communication de documents de toute nature propres à faciliter l’accomplissement de leur mission. Ils peuvent les obtenir ou en prendre copie, par tout moyen et sur tout support, ou procéder à la saisie de ces documents en quelques mains qu’ils se trouvent.

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 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.

# L.1332-14 Code de la défense [nouveau] [coopérer avec l’autorité administrative]

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 à la présente sous‑section, notamment en fournissant des renseignements incomplets ou inexacts, ou en communiquant des pièces incomplètes ou dénaturées, est puni d’une amende administrative prononcée par la commission des sanctions mentionnée à l’article L.1332-15 dont le montant, proportionné à la gravité du manquement, ne peut excéder dix millions d’euros ou, lorsqu’il s’agit d’une entreprise, 2 % du chiffre d’affaires annuel mondial hors taxes de l’exercice précédent, le montant le plus élevé étant retenu.

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

Sous-section 2 Code de la défense - Sanctions

# L.1332-15 Code de la défense [nouveau] [commission des sanctions]

Tout manquement aux dispositions du présent chapitre peut donner lieu aux sanctions prévues à l’article L.133-17, 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.

# L.1332-16 Code de la défense [nouveau] [commission des sanctions]

La commission des sanctions mentionnée à l’article L.1332-15 est composée :

1° D’un membre du Conseil d’État, président, désigné par le vice‑président du Conseil d’État, d’un membre de la Cour de cassation désigné par le premier président de la Cour de cassation, d’un membre de la Cour des comptes désigné par le premier président de la Cour des comptes ;

2° Et de trois personnalités qualifiées nommées respectivement par le Premier ministre, le président de l’Assemblée nationale et le président du Sénat en raison de leurs compétences dans le domaine de la sécurité des activités d’importance vitale.

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

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 mentionnés au 1° ainsi que leurs suppléants respectifs sont nommés par décret.

Le mandat du président, des membres de la commission ainsi que de leurs suppléants respectifs est de cinq ans, renouvelable une fois. Ils sont tenus au secret professionnel.

# L.1332-17 Code de la défense [nouveau] [commission des sanctions]

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

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 au premier alinéa du présent I.

II. – En cas de manquement constaté aux obligations mentionnées à l’article 26 de la loi [résilience], la commission des sanctions, dans la composition prévue à l’article 36 de la même loi, peut prononcer les sanctions prévues aux articles 28 et 37 de ladite loi.

# L.1332-18 Code de la défense [nouveau] [commission des sanctions]

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’État étrangères à l’impôt et au domaine.

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

# L.1332-19 Code de la défense [nouveau] [décret à suivre…]

Les conditions d’application de la présente sous‑section, notamment les règles de fonctionnement de la commission et les modalités de récusation de ses membres, sont définies par décret en Conseil d’État.

Section 3 Code de la défense - Marchés publics et contrats de concession relatifs à la sécurité des activités d’importance vitale

# L.1332-20 Code de la défense [nouveau] [OIV marché publics]

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 :

1° 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’État ;

2° Et que cette protection ou la prévention de ce détournement d’usage ne peuvent être garanties par d’autres moyens.

# L.1332-21 Code de la défense [nouveau] [OIV contrats de concession]

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 :

1° 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’État ;

2° Et que cette protection ou la prévention de ce détournement d’usage ne peuvent être garanties par d’autres moyens.

# L.1332-22 Code de la défense [nouveau] [OIV contrats de concession]

Les opérateurs d’importance vitale qui passent un marché ou un contrat de concession en application des articles L.1332-20 et L.1332-21 en informent l’autorité administrative dans des conditions et des délais précisés par décret.

##### #PJL#Résilience#article#02#

# L.1333-1 Code de la défense [modifié] [matières nucléaires]

Chapitre II - Dispositions diverses

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 » ;

Sont soumises aux dispositions de la présente section les matières nucléaires fusibles, fissiles ou fertiles, ainsi que toute matière, à l'exception des minerais, contenant un ou plusieurs éléments fusibles, fissiles ou fertiles dont la liste est précisée par décret en Conseil d'État.

Les conditions particulières d'application de la présente section aux matières nucléaires affectées aux moyens nécessaires à la mise en œuvre de la politique de dissuasion sont définies par décret en Conseil d'État.

Sont également soumises aux dispositions de la présente section, pour ce qui concerne la protection contre les actes de malveillance, les sources de rayonnements ionisants mises en œuvre par les activités nucléaires réalisées dans certaines infrastructures des opérateurs d’importance vitale mentionnés au 1° du I de l’article L.1332-2, définies par voie réglementaire.

# L.2113-2 Code de la défense [modifié] [OIV ressortissants étrangers]

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

Dans les cas prévus à l'article [L.1111-2](https://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000006071307&idArticle=LEGIARTI000006539645&dateTexte=&categorieLien=cid), des décrets fixent les conditions dans lesquelles les ressortissants étrangers peuvent être admis, sur leur demande écrite, à apporter leur collaboration aux administrations et aux services publics ou aux opérateurs d’importance vitale mentionnés au I de l’article L.1332-2.

La préparation des mesures devant faire l'objet de ces décrets est prévue dans des instructions arrêtées dès le temps de paix, à la diligence des ministres intéressés.

En ce qui concerne l'emploi, comme main-d'œuvre, des ressortissants alliés ou neutres stationnés en France, des instructions déterminent, dès le temps de paix également, les départements ministériels compétents pour régler la situation de ces étrangers :

1° Vis-à-vis des autorités de leur propre pays ;

2° Vis-à-vis des lois et autorités françaises et pour fixer les règles de leur utilisation.

# L.2151-1 Code de la défense [modifié] [service de sécurité nationale]

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

Le service de sécurité nationale est destiné à assurer la continuité de l'action de l'Etat, des collectivités territoriales, et des organismes qui leur sont rattachés, ainsi que des entreprises et établissements dont les activités contribuent à la sécurité nationale.

Le service de sécurité nationale est applicable au personnel 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

Seules les personnes majeures de nationalité française, ressortissantes de l'Union européenne, sans nationalité ou bénéficiant du droit d'asile peuvent être soumises aux obligations du service de sécurité nationale.

# L.2151-4 Code de la défense [modifié] [service de sécurité nationale]

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

Les employeurs mentionnés au deuxième alinéa de [l'article L.2151-1](https://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000006071307&idArticle=LEGIARTI000006539800&dateTexte=&categorieLien=cid) de notifier aux personnes concernées qu'elles sont susceptibles d'être placées sous le régime du service de sécurité nationale.

# L2171-6 Code de la défense [modifié] [service de sécurité nationale]

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

Lors du recours au dispositif de réserve de sécurité nationale, les réservistes sont tenus de rejoindre leur affectation, dans les conditions fixées par les autorités civiles ou militaires dont ils relèvent au titre de leur engagement.

En cas de nécessité inhérente à la poursuite de la production de biens ou de services ou à la continuité du service public, les réservistes employés par un des opérateurs d’importance vitale mentionnés au I de l’article L.1332-2 peuvent être dégagés de ces obligations.

Les conditions de convocation des réservistes sont fixées par décret en Conseil d'État. Ce décret détermine notamment le délai minimal de préavis de convocation.

# L.2321-2-1 Code de la défense [modifié] [OIV marqueurs techniques]

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

Aux seules fins de garantir la défense et la sécurité nationale, lorsqu'elle a connaissance d'une menace susceptible de porter atteinte à la sécurité des systèmes d'information des autorités publiques ou des opérateurs d’importance vitale mentionnés au I de l’article L.1332-2 du présent code ou 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, l'ANSSI peut mettre en œuvre, sur le réseau d'un opérateur de communications électroniques ou sur le système d'information d'une personne mentionnée aux 1 ou 2 du I de l'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique ou d'un opérateur de centre de données :

1° Des dispositifs mettant en œuvre des marqueurs techniques ;

2° Ou, sur avis conforme de l'ARCEP, des dispositifs permettant le recueil de données sur le réseau d'un opérateur de communications électroniques ou sur le système d'information d'une personne mentionnée aux mêmes 1 ou 2 ou d'un opérateur de centre de données affecté par la menace.

Ces dispositifs sont mis en œuvre pour une durée et dans une mesure strictement nécessaires à la caractérisation de la menace et aux seules fins de détecter et de caractériser des événements susceptibles d'affecter la sécurité des systèmes d'information des autorités publiques, des opérateursd’importance vitale mentionnés au I de l’article L.1332-2 du présent code ou à [l'article 5 de la loi n° 2018-133 du 26 février 2018 précitée](https://www.legifrance.gouv.fr/affichTexteArticle.do?cidTexte=JORFTEXT000036644772&idArticle=JORFARTI000036644795&categorieLien=cid)et des opérateurs publics ou privés participant aux systèmes d'information de ces entités.

Les agents de l'ANSSI individuellement désignés et spécialement habilités sont autorisés, aux seules fins de prévenir et de caractériser la menace affectant les systèmes d'information des entités mentionnées au premier alinéa du présent article, à procéder au recueil des données et à l'analyse des seules données techniques pertinentes, à l'exclusion de toute autre exploitation.

Les données directement utiles à la prévention et à la caractérisation des menaces ne peuvent être conservées plus de deux ans. Les autres données recueillies par les dispositifs mentionnés aux 1° et 2° sont détruites dans un délai bref, précisé par voie réglementaire.

Un décret en Conseil d'État, pris après avis de la Commission nationale de l'informatique et des libertés et de l'ARCEP, définit les modalités d'application du présent article. Il détermine notamment les informations et les catégories de données conservées en application du 2°.

# L.2321-3 Code de la défense [modifié] [opérateurs de communications électroniques]

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

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 » ;

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 » ;

Pour les besoins de la sécurité des systèmes d'information des autorités publiques, des opérateurs d’importance vitale mentionné au I de l’article L.1332-2 et des opérateurs mentionnés à l'[article 5 de la loi n° 2018-133 du 26 février 2018](https://www.legifrance.gouv.fr/affichTexteArticle.do?cidTexte=JORFTEXT000036644772&idArticle=JORFARTI000036644795&categorieLien=cid) portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité, les agents de l'ANSSI, habilités par le Premier ministre dans des conditions fixées par décret en Conseil d'État et dont la liste est transmise à l'ARCEP peuvent obtenir des opérateurs de communications électroniques, en application du II bis de l'article L.34-1 [CPCE] et des personnes mentionnées au 2 du I de [l'article 6 de la loi n° 2004-575 du 21 juin 2004](https://www.legifrance.gouv.fr/affichTexteArticle.do?cidTexte=JORFTEXT000000801164&idArticle=LEGIARTI000006421546&dateTexte=&categorieLien=cid) , en application du II du même article 6, l'identité, l'adresse postale et l'adresse électronique d'utilisateurs ou de détenteurs de systèmes d'information vulnérables, menacés ou attaqués, afin de les alerter sur la vulnérabilité ou l'atteinte de leur système.

Lorsque l'ANSSI est informée, en application de l'article L.33-14 du [CPCE], de l'existence d'un événement affectant la sécurité des systèmes d'information d'une autorité publique, d'un opérateur d’importance vitale mentionné au I de l’article L.1332-2 du présent code ou à l'article 5 de la loi n° 2018-133 du 26 février 2018 ou d'un opérateur public ou privé participant aux systèmes d'information d'une des entités mentionnées au présent alinéa, les agents mentionnés au premier alinéa du présent article peuvent obtenir des opérateurs de communications électroniques les données techniques strictement nécessaires à l'analyse de cet événement. Ces données ne peuvent être exploitées qu'aux seules fins de caractériser la menace affectant la sécurité de ces systèmes. Elles ne peuvent être conservées plus de cinq ans.

Les surcoûts identifiables et spécifiques des prestations suivantes effectuées à la demande de l'ANSSI sont compensés selon des modalités prévues par décret en Conseil d'État :

1° Les prestations assurées par les opérateurs de communications électroniques en application du premier alinéa du présent article, dans les conditions prévues au VI de [l'article L.34-1 du [CPCE]](https://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000006070987&idArticle=LEGIARTI000006465770&dateTexte=&categorieLien=cid) , et du deuxième alinéa du présent article ;

2° Les prestations assurées par les personnes mentionnées au 2 du I de l'article 6 de la loi n° 2004-575 du 21 juin 2004.

# L.4231-6 Code de la défense [modifié] [personnes soumises à l'obligation de disponibilité]

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

En cas de nécessité inhérente à la poursuite de la production de biens ou de services ou à la continuité du service public, les personnes soumises à l'obligation de disponibilité employées par des opérateurs d’importance vitale mentionnés au I de l’article L.1332-2 peuvent être dégagées des obligations prévues aux articles L.4231-4 et L.4231-5, dans des conditions fixées par décret en Conseil d'État.

# 226-3 Code pénal [modifié] [dispositifs techniques et sanction pénale]

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 ».

Est puni de cinq ans d'emprisonnement et de 300 000 € d'amende :

1° La fabrication, l'importation, la détention, l'exposition, l'offre, la location ou la vente d'appareils ou de dispositifs techniques de nature à permettre la réalisation d'opérations pouvant constituer l'infraction prévue par le deuxième alinéa de l'article [226-15](https://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000006070719&idArticle=LEGIARTI000006417953&dateTexte=&categorieLien=cid) ou qui, conçus pour la détection à distance des conversations, permettent de réaliser l'infraction prévue par [l'article 226-1](https://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000006070719&idArticle=LEGIARTI000006417928&dateTexte=&categorieLien=cid) ou ayant pour objet la captation de données informatiques prévue aux [articles 706-102-1](https://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000006071154&idArticle=LEGIARTI000023712497&dateTexte=&categorieLien=cid) du code de procédure pénale et [L.853-2](https://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000025503132&idArticle=LEGIARTI000030935966&dateTexte=&categorieLien=cid) du [CSI] et figurant sur une liste dressée dans des conditions fixées par décret en Conseil d'État, lorsque ces faits sont commis, y compris par négligence, en l'absence d'autorisation ministérielle dont les conditions d'octroi sont fixées par ce même décret ou sans respecter les conditions fixées par cette autorisation ;

2° Le fait de réaliser une publicité en faveur d'un appareil ou d'un dispositif technique susceptible de permettre la réalisation des infractions prévues par l'article 226-1 et le deuxième alinéa de l'article 226-15 lorsque cette publicité constitue une incitation à commettre cette infraction ou ayant pour objet la captation de données informatiques prévue aux articles 706-102-1 du code de procédure pénale et [L.853-2 du [CSI]](https://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000025503132&idArticle=LEGIARTI000030935966&dateTexte=&categorieLien=cid) lorsque cette publicité constitue une incitation à en faire un usage frauduleux.

Le présent article n'est pas applicable à la détention ou à l'acquisition par les opérateurs d’importance vitale mentionnés au 1° du I de l’article L.1332-2 Code de la défense, ainsi désignés en vertu de leur activité d'exploitant d'un réseau de communications électroniques ouvert au public, des appareils soumis à une autorisation du Premier ministre en application de la section 7 du chapitre II du titre Ier du livre II du [CPCE].

# L.33-1 CPCE [modifié] [services de communications électroniques]

III. – Le [CPCE] 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 » ;

I. – L'établissement et l'exploitation des réseaux ouverts au public et la fourniture au public de services de communications électroniques sont libres sous réserve du respect de règles portant sur :

a) Les conditions de permanence, de qualité, de disponibilité, de sécurité et d'intégrité du réseau et du service qui incluent des obligations de notification à l'autorité compétente des incidents de sécurité ayant eu un impact significatif sur leur fonctionnement ;

b) Les conditions de confidentialité et de neutralité au regard des messages transmis et des informations liées aux communications ;

c) Les normes et spécifications du réseau et du service ;

d) Les prescriptions exigées par la protection de la santé et de l'environnement et par les objectifs d'aménagement du territoire et d'urbanisme, comportant, le cas échéant, les conditions d'occupation du domaine public, les garanties financières ou techniques nécessaires à la bonne exécution des travaux d'infrastructures, les modalités de partage des infrastructures et des réseaux radioélectriques ouverts au public et d'itinérance locale ;

e) Les prescriptions exigées par l'ordre public, la défense nationale et la sécurité publique, notamment celles qui sont nécessaires à la mise en œuvre des interceptions justifiées par les nécessités de la sécurité publique, ainsi que les garanties d'une juste rémunération des prestations assurées à ce titre et celles qui sont nécessaires pour répondre, conformément aux orientations fixées par l'autorité nationale de défense des systèmes d'informations, aux menaces et aux atteintes à la sécurité des systèmes d'information des autorités publiques et des opérateurs d’importance vitale mentionnés au I de l’article L.1332-2 Code de la défense ;

f) L'acheminement gratuit des communications d'urgence. A ce titre, les opérateurs mettent en œuvre toute mesure permettant de garantir la continuité de l'acheminement de ces communications. Ils sont chargés de mettre en place une supervision technique permettant d'assurer, dans les meilleurs délais, une remontée d'alerte dans les conditions définies par décret. Ils fournissent également gratuitement aux services d'urgence l'information relative à la localisation de l'appelant ;

f bis) L'acheminement gratuit des communications des pouvoirs publics pour alerter la population située dans les zones géographiques potentiellement affectées soit par un cas d'urgence, un accident, un sinistre ou une catastrophe au sens de l'[article L.112-1 [CSI]](https://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000025503132&idArticle=LEGIARTI000025504927&dateTexte=&categorieLien=cid), soit par une menace ou une agression au sens des articles [L.1111-1](https://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000006071307&idArticle=LEGIARTI000006539644&dateTexte=&categorieLien=cid) et [L.1111-2](https://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000006071307&idArticle=LEGIARTI000006539645&dateTexte=&categorieLien=cid) Code de la défense, imminents ou en cours, l'État contribuant aux frais d'équipement en matériels et logiciels acquis spécifiquement pour l'exécution de cette mission ;

f ter) L'acheminement gratuit d'informations d'intérêt général à destination des utilisateurs finals ;

g) Le financement du service universel et, le cas échéant, la fourniture du service universel et des services complémentaires au service universel, dans les conditions prévues aux articles [L.35-2 à L.35-5](https://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000006070987&idArticle=LEGIARTI000006465807&dateTexte=&categorieLien=cid) CPCE ;

h) La fourniture des informations prévues à l'article [L.34](https://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000006070987&idArticle=LEGIARTI000006465404&dateTexte=&categorieLien=cid) CPCE ;

i) L'interconnexion et l'accès, dans les conditions prévues aux articles [L.34-8](https://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000006070987&idArticle=LEGIARTI000006465796&dateTexte=&categorieLien=cid) et [L.38](https://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000006070987&idArticle=LEGIARTI000006465428&dateTexte=&categorieLien=cid) CPCE ;

j) Les conditions nécessaires pour assurer l'équivalence de traitement des opérateurs internationaux conformément aux dispositions du III du présent article ;

k) Les conditions nécessaires pour assurer l'interopérabilité des services ;

l) Les obligations qui s'imposent à l'opérateur pour permettre son contrôle par l'ARCEP et celles qui sont nécessaires pour l'application des articles L.33-12-1 et [L.37-1](https://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000006070987&idArticle=LEGIARTI000006465917&dateTexte=&categorieLien=cid) CPCE ;

m) (Abrogé)

n) L'information des utilisateurs, dans la mesure où cette information est nécessaire à la mise en œuvre des dispositions du présent code ou des décisions prises en application de celui-ci ;

n bis) Les informations devant figurer dans le contrat conclu avec un utilisateur professionnel, à la demande de ce dernier, et comprenant celles mentionnées à [l'article L.121-83](https://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000006069565&idArticle=LEGIARTI000006292140&dateTexte=&categorieLien=cid) code de la consommation relatives aux prestations qu'il a souscrites ;

n ter) L'obligation de mettre à disposition des utilisateurs professionnels les informations mentionnées à [l'article L.121-83-1](https://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000006069565&idArticle=LEGIARTI000024504553&dateTexte=&categorieLien=cid)  code de la consommation, selon les modalités prévues à ce même article ;

o) Un accès des utilisateurs finals handicapés à des services de communications électroniques à un tarif abordable et aux services d'urgence, équivalent à celui dont bénéficie la majorité des utilisateurs finals ;

p) (1) Un accès des utilisateurs finals sourds, malentendants, sourd aveugles et aphasiques à une offre de services de communications électroniques proposée sans surcoût pour l'utilisateur final et incluant, pour les appels passés et reçus, la fourniture d'un service de traduction simultanée écrite et visuelle défini au IV de l'[article 105 de la loi n° 2016-1321](https://www.legifrance.gouv.fr/affichTexteArticle.do?cidTexte=JORFTEXT000033202746&idArticle=LEGIARTI000047293258&dateTexte=&categorieLien=id) du 7 octobre 2016, dans la limite d'un usage raisonnable, dans des conditions définies par décret et dans le respect des conditions de qualité définies par l'ARCEP.

Cette offre répond également, pour les appels passés et reçus, aux exigences d'accessibilité prévues à l'article [L.412-13](https://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000006069565&idArticle=LEGIARTI000047284897&dateTexte=&categorieLien=cid) code de la consommation.

Elle garantit les conditions de neutralité et de confidentialité mentionnées au b du présent I ainsi que la prévention de la violation des données à caractère personnel mentionnée à l'[article 83 de la loi n° 78-17 du 6 janvier 1978](https://www.legifrance.gouv.fr/affichTexteArticle.do?cidTexte=JORFTEXT000000886460&idArticle=LEGIARTI000037810146&dateTexte=&categorieLien=cid) [informatique et libertés] ;

q) La neutralité de l'internet, qui consiste à garantir l'accès à l'internet ouvert régi par le règlement (UE) 2015/2120 du 25 novembre 2015… ;

Les fournisseurs de services de communications interpersonnelles non-fondés sur la numérotation ne sont concernés que par les règles énoncées aux a, b, c, e, f bis, g, k, l, n, n bis, n ter et o du présent I.

Un décret fixe les modalités d'application du présent article, notamment les informations visées aux n bis et n ter, et précise, en tant que de besoin, selon les différentes catégories de réseaux et de services, les règles mentionnées aux a à q.

II. – Les opérateurs réalisant un chiffre d'affaires annuel sur le marché des communications électroniques supérieur à un seuil fixé par arrêté des ministres chargés des communications électroniques et de l'économie sont tenus d'individualiser sur le plan comptable leur activité.

En outre, lorsqu'ils disposent dans un secteur d'activité autre que les communications électroniques d'un monopole ou d'une position dominante appréciée après avis de l'Autorité de la concurrence, et que les infrastructures utilisées peuvent être séparées physiquement, ils sont tenus, dans l'intérêt d'un bon exercice de la concurrence, d'individualiser cette activité sur le plan juridique.

III. – Sous réserve des engagements internationaux souscrits par la France, le ministre chargé des communications électroniques et l'ARCEP veillent à ce que soit assurée l'égalité de traitement des opérateurs acheminant du trafic international au départ ou à destination de réseaux ouverts au public français, notamment dans les conditions d'accès aux réseaux français et étrangers.

Sous la même réserve, ils veillent également à ce que les opérateurs des pays tiers à l'Union européenne assurent aux opérateurs au sens du 15° de l'article L.32 ayant une activité en France des droits comparables, notamment en matière d'interconnexion et d'accès à ceux dont ils bénéficient sur le territoire national, en application du présent code.

IV. – Les installations mentionnées au 2° de l'article [L.33](https://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000006070987&idArticle=LEGIARTI000006465400&dateTexte=&categorieLien=cid) doivent respecter les règles mentionnées aux i et l du I.

V. – Les opérateurs de services de communications électroniques sont tenus de permettre l'accès par les autorités judiciaires, les services de la police et de la gendarmerie nationale, les services d'incendie et de secours et les services d'aide médicale d'urgence, agissant dans le cadre de missions judiciaires ou d'interventions de secours, à leurs listes d'abonnés et d'utilisateurs, complète, non expurgée et mise à jour.

VI.-Les opérateurs n'apportent aucune limitation technique ou contractuelle à un service d'accès à internet, qui aurait pour objet ou effet d'interdire à un utilisateur de ce service qui en fait la demande :

1° D'accéder, depuis un point d'accès à internet, à des données enregistrées sur un équipement connecté à internet, par l'intermédiaire du service d'accès auquel il a souscrit ou de donner à des tiers accès à ces données ;

2° D'accéder au réseau local hertzien de son choix fourni par des tiers ou de permettre l'accès d'autres utilisateurs finals au réseau de ces opérateurs par l'intermédiaire de réseaux locaux hertziens.

VII.-1° Les dispositions du e du I sont applicables en Polynésie française, dans les îles Wallis et Futuna et en Nouvelle-Calédonie dans leur rédaction résultant de l'[ordonnance n° 2021-650 du 26 mai 2021](https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000043534846&categorieLien=cid) portant transposition de la directive (UE) 2018/1972 du 11 décembre 2018 [code des communications électroniques européen] ;

2° Les dispositions du f bis du I sont applicables en Polynésie française et dans les îles Wallis et Futuna dans leur rédaction résultant de l'ordonnance n° 2021-650 du 26 mai 2021 précitée ;

3° Les dispositions du f bis du I sont applicables en Nouvelle-Calédonie dans leur rédaction résultant de l'ordonnance n° 2021-650 du 26 mai 2021 précitée, sous réserve des compétences exercées par cette collectivité en application du statut qui la régit.

# L.33-14 CPCE [modifié] [OIV marqueurs techniques]

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 ».

Pour les besoins de la sécurité et de la défense des systèmes d'information, les opérateurs, d’importance vitale mentionnés au 1° du I de l’article L.1332-2 Code de la défense, ainsi désignés en vertu de leur activité d'exploitant d'un réseau de communications électroniques ouvert au public, recourent, sur les réseaux de communications électroniques qu'ils exploitent, à des dispositifs mettant en œuvre des marqueurs techniques fournis par l'ANSSI aux seules fins de détecter des événements susceptibles d'affecter la sécurité des systèmes d'information de leurs abonnés. Ces dispositifs sont mis en œuvre pour répondre aux demandes de l'ANSSI.

Lorsqu'elle a connaissance d'une menace susceptible de porter atteinte à la sécurité des systèmes d'information, l'ANSSI demande aux opérateurs de communications électroniques d'exploiter les marqueurs techniques qu'elle fournit.

Par dérogation au II de l'article [L.34-1](https://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000006070987&idArticle=LEGIARTI000006465770&dateTexte=&categorieLien=cid), les opérateurs mentionnés au premier alinéa du présent article sont autorisés à conserver, pour une durée maximale de six mois, les données techniques strictement nécessaires à la caractérisation d'un évènement détecté par les dispositifs mentionnés au même premier alinéa. Les données recueillies dans le cadre de l'exploitation de ces dispositifs autres que celles directement utiles à la prévention et à la caractérisation des menaces sont immédiatement détruites.

Lorsque sont détectés des événements susceptibles d'affecter la sécurité des systèmes d'information, les opérateurs mentionnés audit premier alinéa en informent sans délai l'ANSSI.

A la demande de l'ANSSI, les opérateurs mentionnés au même premier alinéa informent leurs abonnés de la vulnérabilité de leurs systèmes d'information ou des atteintes qu'ils ont subies.

Les modalités d'application du présent article sont précisées par décret en Conseil d'État. Celui-ci détermine notamment les catégories de données pouvant être conservées par les opérateurs mentionnés au premier alinéa, les modalités de compensation des surcoûts identifiables et spécifiques des prestations assurées à ce titre par les opérateurs, à la demande de l'ANSSI, ainsi que les garanties d'une juste rémunération pour la mise en place des dispositifs mentionnés au même premier alinéa."

# L.34-11 CPCE [modifié] [connecter les terminaux au réseau radioélectrique mobile]

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 ».

I.-Est soumise à une autorisation du Premier ministre, dans le but de préserver les intérêts de la défense et de la sécurité nationale, l'exploitation sur le territoire national des appareils, à savoir tous dispositifs matériels ou logiciels, permettant de connecter les terminaux des utilisateurs finaux au réseau radioélectrique mobile, à l'exception des réseaux de quatrième génération et des générations antérieures, qui, par leurs fonctions, présentent un risque pour la permanence, l'intégrité, la sécurité, la disponibilité du réseau, ou pour la confidentialité des messages transmis et des informations liées aux communications, à l'exclusion des appareils installés chez les utilisateurs finaux ou dédiés exclusivement à un réseau indépendant, des appareils électroniques passifs ou non configurables et des dispositifs matériels informatiques non spécialisés incorporés aux appareils.

L'autorisation mentionnée au premier alinéa du présent I n'est requise que pour l'exploitation, directe ou par l'intermédiaire de tiers fournisseurs, d'appareils par les opérateurs d’importance vitale mentionnés au 1° du I de l’article L.1332-2 Code de la défense, ainsi désignés en vertu de leur activité d'exploitant d'un réseau de communications électroniques ouvert au public.

La liste des appareils dont l'exploitation est soumise à l'autorisation mentionnée au premier alinéa du présent I est fixée par arrêté du Premier ministre, pris après avis de l'Autorité de régulation des communications électroniques et des postes. Cette liste énumère les différents appareils concernés en référence à la terminologie utilisée dans les standards internationaux associés aux réseaux radioélectriques mobiles de cinquième génération et des générations ultérieures.

II.-L'autorisation d'exploitation d'un appareil peut être octroyée après examen d'un dossier de demande d'autorisation remis par l'opérateur. Le dossier précise les modèles et les versions des appareils pour lesquels l'autorisation est sollicitée.

L'autorisation est octroyée, le cas échéant sous conditions, pour une durée maximale de huit ans. Le renouvellement de l'autorisation fait l'objet d'un dossier de demande de renouvellement, qui est remis au moins deux mois avant l'expiration de l'autorisation en vigueur.

Les modalités d'octroi de l'autorisation, les conditions dont elle peut être assortie ainsi que la composition du dossier de demande d'autorisation et du dossier de demande de renouvellement sont fixées par décret en Conseil d'État, pris après avis de l'Autorité de régulation des communications électroniques et des postes et de la Commission supérieure du numérique et des postes, qui se prononcent dans un délai d'un mois à compter de leur saisine.

# L.1333-9 CSP [modifié] [activités nucléaires à faible exposition aux rayonnements ionisants]

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

I.-Les activités nucléaires susceptibles d'occasionner une faible exposition aux rayonnements ionisants, et répondant à des caractéristiques fixées par voie réglementaire, sont exemptées de l'obligation de déclaration, d'enregistrement ou d'autorisation prévue à l'article L.1333-8.

II.-Les activités nucléaires exercées dans une installation nucléaire de base relevant du régime prévu à l'article L.593-1 du code de l'environnement ne sont pas soumises aux dispositions de l'article L.1333-8.

Ces activités nucléaires sont toutefois soumises, sauf disposition contraire, à la réglementation générale applicable aux activités nucléaires pour la protection des intérêts mentionnés à l'article [L.1333-7](https://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000006072665&idArticle=LEGIARTI000006686676&dateTexte=&categorieLien=cid).

Les actes réglementaires ou individuels pris en application du régime des installations nucléaires de base assurent la prise en compte des obligations prévues par le présent chapitre. Ils tiennent compte de l'autorisation délivrée au titre de l'article [L.1333-2](https://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000006071307&idArticle=LEGIARTI000006539704&dateTexte=&categorieLien=cid) Code de la défense, lorsque l'activité nucléaire bénéficie de moyens et mesures de protection pris en application de la section 1 du chapitre III du titre III du livre III de la première partie du Code de la défense, auquel cas le contrôle de ces moyens et mesures ne relève pas du présent chapitre.

Toutefois, les actes réglementaires et individuels mentionnés ci-dessus ne concernent pas la protection contre les actes de malveillance :

1° Dans les emprises placées sous l'autorité du ministre de la défense ;

2° Dans certaines infrastructures des opérateurs d’importance vitale mentionnés au 1° du I de l’article L.1332-2 du Code de la défense déterminés par voie réglementaire ;

3° Pour les sources de rayonnements ionisants qui sont également des matières nucléaires soumises à autorisation en application de l'article L.1333-2 Code de la défense.

Dans les cas relevant du 2° et du 3° ne relevant pas également du 1°, la prise en compte des obligations en matière de protection contre les actes de malveillance est assurée par le régime d'autorisation prévu au L.1333-2 Code de la défense.

III.-Les activités nucléaires définies dans la nomenclature prévue à l'article [L.511-2](https://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000006074220&idArticle=LEGIARTI000006834229&dateTexte=&categorieLien=cid)  code de l'environnement ou relevant en elles-mêmes de l'application de l'article [L.162-1](https://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000023501962&idArticle=LEGIARTI000023504885&dateTexte=&categorieLien=cid)  code minier ne sont pas soumises aux dispositions de l'article L.1333-8.

Ces activités nucléaires sont toutefois soumises, sauf disposition contraire, à la réglementation générale applicable aux activités nucléaires pour la protection des intérêts mentionnés à l'article L.1333-7.

Les actes réglementaires ou individuels pris en application des régimes mentionnés au premier alinéa du présent III assurent la prise en compte des obligations prévues par le présent chapitre, à l'exception de celles relatives à la protection contre les actes de malveillance.

Au titre de la protection contre les actes de malveillance, certaines de ces activités nucléaires sont soumises à une autorisation délivrée par l'Autorité de sûreté nucléaire et de radioprotection dans les conditions prévues à l'article [L.1333-8](https://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000006072665&idArticle=LEGIARTI000006686680&dateTexte=&categorieLien=cid). Cette autorisation tient compte de celle délivrée au titre de l'article L.1333-2 du Code de la défense, lorsque l'activité nucléaire bénéficie de moyens et mesures de protection pris en application de la section 1 du chapitre III du titre III du livre III de la première partie du Code de la défense, auquel cas le contrôle de ces moyens et mesures ne relève pas du présent chapitre.

Toutefois, l'alinéa précédent ne s'applique pas :

1° Dans les emprises placées sous l'autorité du ministre de la défense ;

2° Dans certains établissements, installations ou ouvrages relevant de l'article [L.1332-1](https://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000006071307&idArticle=LEGIARTI000006539687&dateTexte=&categorieLien=cid) du Code de la défense définis par voie réglementaire ;

3° Pour les sources de rayonnements ionisants qui sont également des matières nucléaires soumises à autorisation en application de l'article L.1333-2 du Code de la défense.

Dans les cas 2° et 3° ne relevant pas également du 1°, la prise en compte des obligations en matière de protection contre les actes de malveillance est assurée par le régime d'autorisation prévu au L.1333-2 du Code de la défense.

IV.-Les activités nucléaires exercées dans les installations et activités nucléaires intéressant la défense mentionnées à l'article L.1333-15 du Code de la défense ne sont pas soumises aux dispositions de l'article L.1333-8.

Ces activités nucléaires peuvent faire l'objet de dispositions réglementaires particulières adaptant la réglementation générale applicable aux activités nucléaires pour la protection des intérêts mentionnés à l'article L.1333-7.

Les actes réglementaires ou individuels pris en application des régimes applicables à ces installations et activités assurent la prise en compte des obligations prévues par le présent chapitre.

V.-L'autorisation mentionnée à l'article L.1333-8 tient compte de celle délivrée au titre de l'article L.1333-2 du Code de la défense, lorsque l'activité nucléaire bénéficie de moyens et mesures de protection pris en application de la section 1 du chapitre III du titre III du livre III de la première partie du Code de la défense, auquel cas le contrôle de ces moyens et mesures ne relève pas du présent chapitre.

VI.-Le régime mentionné à l'article L.1333-8 ne porte pas sur les obligations en matière de protection contre les actes de malveillance dans les cas suivants :

1° Dans les emprises et pour les transports de substances radioactives placés sous l'autorité du ministre de la défense à destination ou en provenance de ces emprises ;

2° Dans certaines infrastructures des opérateurs d’importance vitale mentionnés au 1° du I de l’article L.1332-2 du Code de la défense définis par voie réglementaire ;

3° Pour les sources de rayonnements ionisants qui sont également des matières nucléaires soumises à autorisation en application de l'article L.1333-2 du Code de la défense ;

4° Pour les transports de substances radioactives soumis au régime défini à l'article L.1333-2 du Code de la défense.

Ces activités nucléaires peuvent faire l'objet de dispositions réglementaires particulières adaptant la réglementation générale applicable aux activités nucléaires en matière de protection contre les actes de malveillance.

Dans les cas 2°, 3° et 4° ne relevant pas également du 1°, la prise en compte des obligations en matière de protection contre les actes de malveillance est assurée par le régime d'autorisation prévu au L.1333-2 du Code de la défense.

# L.223-2 CSI [modifié] [systèmes de vidéoprotection]

V. – Le [CSI] 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 » ;

Aux fins de prévention d'actes de terrorisme, le représentant de l'État dans le département et, à Paris, le préfet de police peuvent prescrire la mise en œuvre, dans un délai qu'ils fixent, de systèmes de vidéoprotection, aux personnes suivantes :

1° Les opérateurs d’importance vitale mentionnés au I de l’article L.1332-2 du Code de la défense ;

2° Les gestionnaires d'infrastructures, les autorités et personnes exploitant des transports collectifs, relevant de l'activité de transports terrestres régie par l'article [L.1000-1](https://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000023086525&idArticle=LEGIARTI000023068937&dateTexte=&categorieLien=cid) du code des transports ;

3° Les exploitants d'aéroports qui, n'étant pas mentionnés aux deux alinéas précédents, sont ouverts au trafic international.

# L.223-8 CSI [modifié] [systèmes de vidéoprotection]

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

Aux fins de prévention d'actes de terrorisme, de protection des abords des infrastructures des opérateurs d’importance vitale mentionnés au I de l’article L.1332-2 du Code de la défense ou de protection des intérêts fondamentaux de la Nation, le représentant de l'État dans le département ou, à Paris, le préfet de police, peut demander à une commune la mise en œuvre de systèmes de vidéoprotection. Le conseil municipal doit en délibérer dans un délai de trois mois.

Les conditions de financement du fonctionnement et de la maintenance du système de vidéoprotection font l'objet d'une convention conclue entre la commune de son lieu d'implantation et le représentant de l'État dans le département ou, à Paris, le préfet de police.

Les articles [L.223-3](https://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000025503132&idArticle=LEGIARTI000025505242&dateTexte=&categorieLien=cid) et [L.223-5](https://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000025503132&idArticle=LEGIARTI000025505246&dateTexte=&categorieLien=cid) sont applicables.

# 15 loi n°2006-961 [modifié] [mesures techniques logicielles]

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 ».

L'importation, le transfert depuis un État membre de la Union européenne, la fourniture ou l'édition de logiciels susceptibles de traiter des œuvres protégées et intégrant des mesures techniques permettant le contrôle à distance direct ou indirect d'une ou plusieurs fonctionnalités ou l'accès à des données à caractère personnel sont soumis à une déclaration préalable auprès du service de l'État chargé de la sécurité des systèmes d'information. Le fournisseur, l'éditeur ou la personne procédant à l'importation ou au transfert depuis un État membre de l'Union européenne est tenu, à la demande de ce service, de transmettre à celui-ci les spécifications et le code source des logiciels concernés, le code source des bibliothèques utilisées lorsque celui-ci est disponible, ainsi que l'ensemble des outils et méthodes permettant l'obtention de ces logiciels à partir des codes source fournis. Le service de l'État chargé de la sécurité des systèmes d'information peut, si ces logiciels s'appuient sur des bibliothèques et composants logiciels créés, importés ou conçus par une tierce partie, demander à celle-ci la fourniture des mêmes éléments. Un décret en Conseil d'État fixe les conditions dans lesquelles sont souscrites ces déclarations et transmises les informations techniques visées ci-dessus.

Les logiciels visés au premier alinéa ne peuvent être utilisés dans des systèmes de traitement automatisé de données dont la mise en œuvre est nécessaire à la sauvegarde des droits afférents aux œuvres protégées que lorsqu'ils sont opérés dans le respect des dispositions de la [loi n° 78-17 du 6 janvier 1978](https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000886460&categorieLien=cid) [informatique et libertés] et dans des conditions ne portant notamment pas atteinte aux secrets protégés par la loi, ni à l'ordre public.

L'État est autorisé à déterminer les conditions dans lesquelles les logiciels visés au premier alinéa peuvent être utilisés dans les systèmes de traitement automatisé de données des administrations de l'État, des collectivités territoriales et des opérateurs d’importance vitale mentionnés au I de l’article L.1332-2 du Code de la défense.

Un décret en Conseil d'État fixe les conditions d'application du présent article ainsi que la nature des systèmes de traitement automatisé de données auxquels elles s'appliquent.

##### #PJL#Résilience#article#03#

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 :

# L.6221-2 Code de la défense [nouveau] [St-Barthélémy]

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

# L.6222-1 Code de la défense [nouveau] [St-Barthélémy]

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

# L.6242-2 Code de la défense [nouveau] [St-Pierre-et-Miquelon]

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

# L.6312-3 Code de la défense [nouveau] [Wallis-et-Futuna etc.]

II. – L’article 711-1 du code pénal est ainsi rédigé :

# 711-1 code pénal [ré-écrit] [Wallis-et-Futuna etc.]

III. – Le chapitre II du titre Ier du livre II [CPCE] est ainsi modifié :

Chapitre III - Dispositions transitoires

##### #PJL#Résilience#article#04# [décret pour entrée en vigueur]

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

Les opérateurs d’importance vitale désignés avant la date d’entrée en vigueur 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 leur sont applicables avant la date d’entrée en vigueur du titre Ier 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'ANSSI

##### #PJL#Résilience#article#05# [modifié Sénat] [ANSSI]

L'ANSSI mentionnée à l’article L.2321-1 du Code de la défense est chargée de la mise en œuvre de la politique du Gouvernement en matière de sécurité des systèmes d’information régie par le présent titre et de son contrôle.

Le Premier ministre peut désigner un organisme autre que l'ANSSI 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’État. Ces missions comprennent notamment l’accompagnement et le soutien au développement de la filière cybersécurité en coordination avec les ministères compétents.

##### #PJL#Résilience#article#05bis# [nouveau Sénat] [stratégie nationale de cybersécurité]

Afin de parvenir à un niveau élevé de cybersécurité et de le maintenir, le Premier ministre élabore une stratégie nationale en matière de cybersécurité, qui comprend notamment :

1° Les objectifs et priorités de la Nation en matière de cybersécurité, couvrant en particulier les secteurs mentionnés à l’article 7 ;

2° Une liste des différents acteurs et autorités concernés par la mise en œuvre de la stratégie nationale en matière de cybersécurité ;

3° Un cadre de gouvernance visant une coordination renforcée entre les acteurs et autorités définis au 2° dans le but d’atteindre les objectifs et priorités mentionnés au 1° ;

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

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

5° Un plan comprenant les mesures nécessaires en vue d’améliorer le niveau général de sensibilisation des entreprises, des administrations publiques et des citoyens à la cybersécurité ;

5° bis Les modalités de soutien aux collectivités territoriales et à leurs groupements ;

5° ter L’identification et le renforcement des compétences et des formations nécessaires sur l’ensemble du territoire ;

6° Les indicateurs clés de performance aux fins de l’évaluation de la mise en œuvre de la stratégie nationale en matière de cybersécurité.

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

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

Chapitre II De la cyber‑résilience

Section 1 - Définitions

##### #PJL#Résilience#article#06# [modifié Sénat] [NIS2 définitions légales]

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 ;

2° bis **Incident** : un événement compromettant la disponibilité, l’authenticité, l’intégrité ou la confidentialité des données stockées, transmises ou faisant l’objet d’un traitement, ou des services que les réseaux et systèmes d’information offrent ou rendent accessibles ;

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 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 services de confiance qualifié** : un prestataire de services de confiance au sens du paragraphe 20 de l’article 3 du règlement (UE) n° 910/2014 du 23 juillet 2014 précité ;

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 application 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 ;

8°**Vulnérabilité** : une faiblesse, susceptibilité ou faille de produits ou services des technologies de l’information et de la communication, ou d’un utilisateur de ces derniers, qui peut être exploitée par une cybermenace.

Section 2 - Des exigences de sécurité des systèmes d’information

##### #PJL#Résilience#article#07# [ré-écrit Sénat] [NIS2 secteurs [hautement] critiques]

~~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’État.~~

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

1° De l’énergie ;

2° Des transports ;

3° Des banques ;

4° Des infrastructures des marchés financiers ;

5° De la santé ;

6° De l’eau potable ;

7° Des eaux usées ;

8° De l’infrastructure numérique ;

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

10° De l’espace.

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

1° Des services postaux et d’expédition ;

2° De la gestion des déchets ;

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

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

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

6° Des fournisseurs de certains services numériques ;

7° De la recherche.

III. – Un décret en Conseil d’État précise les modalités d’application du présent article. Il détermine les sous‑secteurs et les types d’entités relevant des secteurs mentionnés aux I et II.

##### #PJL#Résilience#article#08 [modifié Sénat] [NIS2 entités essentielles #EE]

Sont des entités essentielles :

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

2° Les établissements publics à caractère industriel et commercial, à l’exception du CEA 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 [CGCT], relevant d’un type d’entités appartenant à un des secteurs d’activité hautement critiques, qui emploient au moins 250 personnes **ou** dont les produits d’exploitation excèdent 50 millions d’euros **et** le total du bilan annuel excède 43 millions d’euros. Le critère d’emploi est calculé selon les modalités prévues au I de l’article L.130-1 [CSS], 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 services 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’État et leurs établissements publics administratifs, à l’exception des administrations de l’État qui exercent leurs activités dans les domaines de la sécurité publique, de la défense et de la sécurité nationale, de la répression pénale et des missions diplomatiques et consulaires françaises pour leurs réseaux et systèmes d’information ainsi que de leurs établissements publics administratifs qui exercent leurs activités dans les mêmes domaines ou qui sont désignés entité importante par arrêté du Premier ministre. Le Premier ministre désigne par arrêté les établissements publics administratifs de l’État qui, compte tenu du faible impact économique et social de leur activité, ne sont pas soumis à la présente loi, dans des conditions précisées par décret en Conseil d’État ;

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 [CGFP] ;

d) Les services départementaux d’incendie et de secours mentionnés à l’article L.1424-1 [CGCT] ;

e) Les communautés urbaines, les communautés d’agglomération comprenant au moins une commune de plus de 30.000 habitants 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 [CGCT] 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 [CGCT] 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 [CRPA], à compétence nationale, à l’exception de ceux qui sont désignés entité importante par arrêté du Premier ministre. Le Premier ministre désigne par arrêté les organismes et personnes morales qui, compte tenu du faible impact économique et social de leur activité, ne sont pas soumis à la présente loi, dans des conditions précisées par décret en Conseil d’État ;

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

9° Les opérateurs de services essentiels désignés en application de l’article 5 de la loi n° 2018-133 du 26 février 2018 … 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’État, qui remplissent l’un des critères mentionnés à l’article 10 [PJL Résilience].

##### #PJL#Résilience#article#09# [modifié Sénat] [NIS2 entités importantes #EI]

Sont des entités importantes :

1° Les entreprises relevant d’un type d’entités 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 d’agglomération ne comprenant pas au moins une commune de plus de 30.000 habitants, 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 des conditions précisées par décret en Conseil d’État ;

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

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 [CRPA], à compétence nationale, expressément désignés en tant qu’entités importantes par arrêté du Premier ministre dans des conditions précisées par décret en Conseil d’État ;

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 [CGCT], relevant d’un type d’entités appartenant à un des secteurs d’activité hautement critiques ou critiques, qui emploient au moins 50 personnes ou dont le produit d’exploitation et le total du bilan annuel excèdent chacun 10 millions d’euros et qui ne sont pas entités essentielles. Le critère d’emploi est calculé selon les modalités prévues au I de l’article L.130-1 [CSS], les critères financiers sont appréciés au niveau de la personne morale ou de la régie concernée.

##### #PJL#Résilience#article#10# [NIS2 #EE #EI désignation dérogatoire par PM]

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.

##### #PJL#Résilience#article#11# [NIS2 #EE #EI territoire national

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 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**.

##### #PJL#Résilience#article#12# [modifié Sénat] [NIS2 liste #EE #EI]

L'ANSSI établit et met à jour au moins tous les deux ans 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’État.~~

Dans le respect des modalités de chiffrement de bout en bout ainsi que de protection des données recueillies de l’effet des lois extraterritoriales, les informations à transmettre, leurs modalités de communication et les délais dans lesquels les modifications doivent être transmises sont définis par décret en Conseil d’État.

##### #PJL#Résilience#article#13# [NIS2 et actes sectoriels]

Les dispositions 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'ANSSI.

##### #PJL#Résilience#article#14# [modifié Sénat] [NIS2 mesures opérationnelles]

Les entités essentielles, les entités importantes, les administrations de l’État et leurs établissements publics administratifs qui exercent leurs activités dans les domaines de la **sécurité publique, de la défense et de la sécurité nationale ainsi que de la répression pénale**, les missions diplomatiques et consulaires françaises pour leurs réseaux et systèmes d’information, le CEA 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 [SI] adaptée, comprenant notamment la formation à la cybersécurité des membres des organes de direction et des personnes exposées aux risques;~~

1° Prévoir que les organes de direction approuvent et supervisent les mesures de pilotage de la sécurité des réseaux et systèmes d’information, leurs membres ainsi que les personnes exposées aux risques devant être formés à la cybersécurité ;

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’État 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, en fonction de leur degré d’exposition aux risques, de leur taille, de la probabilité de survenance d’incidents et de leur gravité, y compris leurs conséquences économiques et sociales, et les modalités de concertation des représentants des entités concernées et des associations d’élus.

Ce référentiel peut prescrire le recours à des produits, des services ou des processus certifiés au titre du règlement (UE) n° 2019/881 [ENISA].

Par dérogation aux sixième et septième alinéas du présent article, lorsqu’ils sont des entités importantes ou essentielles, les fournisseurs de services de systèmes de noms de domaine, les offices d’enregistrement, les fournisseurs de services d’informatique en nuage, les fournisseurs de services de centres de données, les fournisseurs de réseaux de diffusion de contenu, les fournisseurs de services gérés, les fournisseurs de services de sécurité gérés, ainsi que les fournisseurs de places de marché en ligne, de moteurs de recherche en ligne et de plateformes de services de réseaux sociaux et les prestataires de services de confiance mettent en œuvre les exigences techniques et méthodologiques qui leur sont propres. [NDLR = REX NIS2 du 17 octobre 2024]

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

##### #PJL#Résilience#article#15# [modifié Sénat] [NIS2 référentiel d'exigences]

Les personnes mentionnées à l’article 14 qui mettent en œuvre les exigences du référentiel mentionné au sixième alinéa du même article 14 ou qui mettent en œuvre tout autre référentiel reconnu comme équivalent par l'ANSSI peuvent s’en prévaloir auprès de celle-ci lors d’un contrôle pour démontrer le respect des objectifs mentionnés au même sixième alinéa, le cas échéant au moyen d’un label de confiance approuvé par elle.

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.

##### #PJL#Résilience#article#16# [OIV liste des SIIV]

Les opérateurs mentionnés à l’article L.1332-2 du Code de la défense identifient, tiennent à jour et communiquent à l'ANSSI la liste de leurs systèmes d’information d’importance vitale mentionnés au 2° de l’article L.1332-1 du même code selon des 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 de la présente loi 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’État et leurs établissements publics administratifs qui exercent leurs activités dans les domaines de la sécurité publique, de la défense et de la sécurité nationale, de la répression pénale, ou des missions diplomatiques et consulaires françaises 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 mettent en œuvre les exigences du référentiel mentionné au même 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 premier à troisième alinéas du présent article peuvent prescrire le recours à des dispositifs matériels ou logiciels ou à des prestataires de services certifiés, qualifiés ou agréés ou prévoir que 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.

##### #PJL#Résilience#article#16bis# [nouveau Sénat] [chiffrement et backdoor]

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

##### #PJL#Résilience#article#17# [modifié Sénat] [NIS2 notification des incidents de sécurité]

Les personnes mentionnées à l’article 14 notifient sans retard injustifié à l'ANSSI tout incident ayant un impact important sur la fourniture de leurs services.

Un incident est considéré comme important si :

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

2° Il a affecté ou est susceptible d’affecter d’autres personnes physiques ou morales en causant des dommages matériels, corporels ou moraux considérables.

Les personnes mentionnées au même article 14 soumettent à l'ANSSI :

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

b) Sans retard injustifié et au plus tard dans les soixante‑douze heures après avoir eu connaissance de l’incident important, une notification intermédiaire qui, le cas échéant, met à jour les informations mentionnées au a, et fournit une évaluation initiale de l’incident important, y compris de sa gravité et de son impact, ainsi que des indicateurs de compromission lorsqu’ils sont disponibles. Par dérogation, les entités mentionnées au 4° de l’article 8 et au 3° de l’article 9 procèdent à cette notification sans retard injustifié et au plus tard dans les vingt‑quatre heures après avoir eu connaissance de l’incident important ayant un impact sur la fourniture de leurs services de confiance ;

c) À la demande de l'ANSSI, un rapport sur les mises à jour pertinentes de la situation ;

d) Au plus tard un mois après la notification intermédiaire mentionnée au b, un rapport final, sous réserve que l’incident soit traité ;

e) Dans le cas contraire, un rapport d’avancement, au plus tard un mois après la notification intermédiaire mentionnée au même b, devant être complété par un rapport final dans un délai d’un mois après le traitement de l’incident.

L'ANSSI fournit, sans retard injustifié et si possible dans les vingt‑quatre heures suivant la réception de la première notification reçue, une réponse à la personne émettrice de la notification.

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'ANSSI peut, après avoir consulté l’entité essentielle ou importante concernée, exiger de celle‑ci qu’elle informe le public de l’incident ou le faire elle‑même.

Le cas échéant, les entités essentielles et importantes notifient sans retard injustifié :

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

– 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 important ou de vulnérabilité critique, les personnes mentionnées au premier alinéa peuvent communiquer à l'ANSSI 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'ANSSI 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’État fixe les modalités d’application du présent article. Il précise notamment la procédure applicable et les critères d’appréciation des caractères importants et critiques des incidents et vulnérabilités.

Section 3 - Enregistrement des noms de domaine

##### #PJL#Résilience#article#18# [offices et bureaux d’enregistrement]

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.

##### #PJL#Résilience#article#19# [offices et bureaux d’enregistrement]

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. À 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’État, pris après avis de la Commission nationale de l’informatique et des libertés, fixe la liste des données relatives aux noms de domaine devant être collectées.

##### #PJL#Résilience#article#20# [modifié Sénat] [offices et bureaux d’enregistrement]

Les offices et les bureaux d’enregistrement conservent les données relatives à chaque nom de domaine dans leur base de données pendant la durée d’utilisation du nom de domaine et jusqu’à expiration d’un délai d’un an à compter de la cessation de l’utilisation de ce nom de domaine.

##### #PJL#Résilience#article#21# [offices et bureaux d’enregistrement]

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.

##### #PJL#Résilience#article#22# [offices et bureaux d’enregistrement]

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'ANSSI 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’État, 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

##### #PJL#Résilience#article#23# [modifié Sénat] [coopération et échange d’informations]

Les dispositions de l’article 11 CPP ou celles relatives aux autres secrets protégés par la loi ne font pas obstacle à la communication d’informations dont ils disposent aux fins de l’accomplissement de leurs missions respectives, à l’exception des informations dont la communication porterait atteinte à la sécurité publique, à la défense et la sécurité nationale ou à la conduite des relations internationales, entre, d’une part, l'ANSSI, et, d’autre part, la 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 États 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.

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

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

##### #PJL#Résilience#article#24# [agrément ANSSI pour prévention et gestion des incidents]

L'ANSSI 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’État.

Chapitre III De la supervision

##### #PJL#Résilience#article#25# [mesures imposées par l'ANSSI]

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'ANSSI peut prescrire à la personne ou au bureau d’enregistrement concerné les mesures nécessaires pour éviter un incident ou y remédier et déterminer les délais accordés pour les mettre en œuvre et en rendre compte.

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

Section 1 - Recherche et constatations des manquements

Sous‑section 1 - Habilitation

##### #PJL#Résilience#article#26A#

# L.103 CPCE [modifié Sénat] [service de coffre-fort numérique]

À l’avant‑dernier alinéa de l’article L.103 du [CPCE], les mots : « établie selon un » sont remplacés par les mots : « lorsqu’il répond aux prescriptions d’un ».

Un service de coffre-fort numérique est un service qui a pour objet :

1° La réception, le stockage, la suppression et la transmission de données ou documents électroniques dans des conditions permettant de justifier de leur intégrité et de l'exactitude de leur origine ;

2° La traçabilité des opérations réalisées sur ces documents ou données et la disponibilité de cette traçabilité pour l'utilisateur ;

3° L'identification de l'utilisateur lors de l'accès au service par un moyen d'identification électronique respectant l'article [L. 102](https://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000006070987&idArticle=LEGIARTI000006465958&dateTexte=&categorieLien=cid) ;

4° De garantir l'accès exclusif aux documents électroniques, données de l'utilisateur ou données associées au fonctionnement du service à cet utilisateur, aux tiers autres que le prestataire de service de coffre-fort numérique, explicitement autorisés par l'utilisateur à accéder à ces documents et données et, le cas échéant, au prestataire de service de coffre-fort numérique réalisant un traitement de ces documents ou données au seul bénéfice de l'utilisateur et après avoir recueilli son consentement dans le respect de la loi n° [78-17](https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000886460&categorieLien=cid) du 6 janvier 1978 [informatique et libertés] ;

5° De donner la possibilité à l'utilisateur de récupérer les documents et les données stockées dans un standard ouvert aisément réutilisable et exploitable par un système de traitement automatisé de données, sauf dans le cas des documents initialement déposés dans un format non ouvert ou non aisément réutilisable qui peuvent être restitués dans leur format d'origine, dans des conditions définies par décret.

Le service de coffre-fort numérique peut également proposer des services de confiance au sens du règlement (UE) n° 910/2014 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.

Ce service de coffre-fort numérique peut bénéficier d'une certification ~~établie selon un~~ lorsqu’il répond aux prescriptions d’un cahier des charges proposé par l'autorité nationale de la sécurité des systèmes d'information après avis de la Commission nationale de l'informatique et des libertés et approuvé par arrêté du ministre chargé du numérique.

Les modalités de mise en œuvre du service de coffre-fort numérique et de sa certification par l'Etat sont définies par décret en Conseil d'État pris après avis de la Commission nationale de l'informatique et des libertés.

##### #PJL#Résilience#article#26# [modifié Sénat] [rechercher et constater les manquements]

Les agents et personnels spécialement désignés et assermentés de l'ANSSI et des services de l’État désignés par elle sont habilités à rechercher et à constater les manquements aux obligations, prescriptions et exigences prévues :

1° Par le règlement (UE) n° 910/2014 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° Par le règlement (UE) n° 2019/881 [ENISA] ;

3° Aux chapitres II et III du présent titre ;

4° À l’article L.100, aux III et IV de l’article L.102 et à l’avant‑dernier alinéa de l’article L.103 du [CPCE] ;

5° Par les exigences de cybersécurité résultant des autorisations, certifications, qualifications et agréments délivrés par l'ANSSI ou, le cas échéant, par les organismes d’évaluation de la conformité.

Les agents et personnels des organismes indépendants ou experts spécialement habilités par l'ANSSI peuvent concourir à la recherche des manquements mentionnés au premier alinéa du présent article sous le contrôle des agents et personnels mentionnés au même premier alinéa.

Sous‑section 2 - Des pouvoirs

##### #PJL#Résilience#article#27# [modifié Sénat] [contrôle ANSSI]

La personne faisant l’objet d’un contrôle de l'ANSSI met à disposition des agents et personnels mentionnés à l’article 26 les moyens nécessaires pour vérifier sur pièces et sur place le respect des obligations mentionnées au même article 26.

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

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 ;

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

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 exploitables 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, qui doit comporter les questions auxquelles il est répondu. Les personnes entendues procèdent elles-mêmes à sa lecture, peuvent y faire consigner leurs observations et y apposent leur signature. Si elles déclarent ne pas pouvoir lire, lecture leur en est faite préalablement à la signature. En cas de refus de signer le procès‑verbal, mention en est faite sur celui‑ci.

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

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

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

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

##### #PJL#Résilience#article#28# [contrôle ANSSI et coopération]

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

Le fait, pour la personne contrôlée, de faire obstacle aux contrôles, notamment en fournissant des renseignements incomplets ou inexacts ou en communiquant des pièces incomplètes ou dénaturées, est constitutif d’un manquement et puni d’une amende administrative prononcée par la commission des sanctions mentionnée à l’article L.1332-15 du Code de la défense, dont le montant, proportionné à la gravité du manquement, ne peut excéder dix millions d’euros ou 2 % du chiffre d’affaires annuel mondial, hors taxes, de l’exercice précédent de l’entreprise à laquelle appartient la personne contrôlée, le montant le plus élevé étant retenu.

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

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

##### #PJL#Résilience#article#29# [modifié Sénat] [contrôle de l'ANSSI]

Le contrôle de l'ANSSI peut prendre les formes suivantes :

1° Inspections sur place et contrôles à distance ;

2° Audits de sécurité réguliers et ciblés réalisés par l'ANSSI ;

2° bisAudits de sécurité réguliers et ciblés réalisés par un organisme indépendant désigné par l'ANSSI ;

3° Scans de sécurité ;

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

Le coût des mesures mentionnées aux 1°, 2°, 3° et 4° est à la charge de l'ANSSI. Celui des mesures mentionnées au 2° bis est à la charge de la personne contrôlée sauf, lorsque les circonstances l’exigent, si l'ANSSI en décide autrement.

##### #PJL#Résilience#article#30# [contrôle de l'ANSSI et décret à suivre…]

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

Section 2 - Mesures consécutives aux contrôles

##### #PJL#Résilience#article#31# [procédure de contrôle]

Lorsqu’un manquement ou une suspicion de manquement aux obligations mentionnées à l’article 26 apparaît au terme d’un contrôle réalisé en application de la section 1, l'ANSSI peut ouvrir une procédure. Le cas échéant, elle en informe la personne contrôlée.

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

Lorsque les faits constatés ne justifient pas l’adoption d’une mesure d’exécution mentionnée aux 1° à 5° du présent article, l'ANSSI clôt la procédure et en informe la personne contrôlée.

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

1° Prononcer un avertissement à son encontre ;

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

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

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

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

La mesure d’exécution adoptée est notifiée à la personne contrôlée et peut être assortie d’une astreinte dont le montant ne peut excéder 5 000 euros par jour de retard.

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

##### #PJL#Résilience#article#32# [supprimé Sénat] [procédure de contrôle]

~~Lorsque cette instruction ne fait pas état de faits justifiant une mesure d’exécution, l’ANSSI clôt la procédure et en informe la personne concernée.~~

~~Dans le cas contraire, l’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~~.

##### #PJL#Résilience#article#33# [modifié Sénat] [procédure de contrôle]

Lorsque la personne contrôlée fournit des éléments montrant qu’elle s’est mise en conformité avec la mesure d’exécution notifiée en application de l’article 31 dans le délai imparti, l'ANSSI constate qu’il n’y a pas lieu de poursuivre la procédure et en informe la personne contrôlée.

Dans le cas contraire, l'ANSSI notifie à la personne contrôlée les griefs retenus à son encontre et saisit la commission des sanctions mentionnée à l’article L.1332-15 du Code de la défense.

Lorsque la personne contrôlée est une entité essentielle au sens des articles 8 et 10 de la présente loi et qu’elle n’apporte pas la preuve qu’elle s’est mise en conformité avec les mesures d’exécution mentionnées aux 2°, 3° et 5° de l’article 31 de la présente loi dans le délai imparti, l'ANSSI 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 celle-ci ait mis un terme au manquement. Lorsque cette certification ou cette autorisation a été délivrée par un organisme de certification ou d’autorisation tiers, l'ANSSI enjoint à cet organisme de la suspendre jusqu’à ce que l’entité ait mis un terme au manquement.

##### #PJL#Résilience#article#34# [procédure de contrôle : décret à suivre…]

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

Section 3 - Des sanctions

##### #PJL#Résilience#article#35# [commission des sanctions]

Saisie par l'ANSSI, 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.

##### #PJL#Résilience#article#36# [modifié Sénat] [commission des sanctions]

Lorsqu’elle est saisie par l'ANSSI de manquements aux obligations découlant de l’application des chapitres II et III du présent titre, la commission des sanctions mentionnée à l’article L.1332-15 du Code de la défense est composée :

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

2° De trois personnalités qualifiées, nommées respectivement par le Premier ministre, le président de l’Assemblée nationale et le président du Sénat en raison de leurs compétences dans le domaine de la sécurité des systèmes d’information. Ces personnalités ne peuvent avoir exercé, au cours des trois années précédant leur nomination, une activité ni au sein de l’une des personnes mentionnées aux articles 8 et 9 ni au sein de l'ANSSI.

##### #PJL#Résilience#article#37# [modifié Sénat] [sanctions possibles]

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

1° À l’encontre des entités essentielles et des opérateurs mentionnés à l’article L.133-2 du Code de la défense, à l’exception des administrations de l’État et de ses établissements publics administratifs, des collectivités territoriales, de leurs groupements et de leurs établissements publics administratifs, une amende administrative dont le montant, proportionné à la gravité du manquement, ne peut excéder 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° À l’encontre des entités importantes, à l’exception des administrations de l’État et de ses établissements publics administratifs, des collectivités territoriales, de leurs groupements et de leurs établissements publics administratifs, une amende administrative dont le montant, proportionné à la gravité du manquement, ne peut excéder 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° À 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 [CPCE] 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 [RGPD], donnant lieu à une amende administrative prononcée par la Commission nationale de l’informatique et des libertés en application des articles 20 à 22-1 de la loi n° 78-17 du 6 janvier 1978, 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’État, des prestataires de services de confiance établis sur le territoire français, des fournisseurs de dispositifs de création de signature et de cachet électronique qualifié qu’elle certifie et des organismes d’évaluation de la conformité, à l’exception des administrations de l’État et de leurs établissements publics à caractère administratif, en cas de manquement constaté au règlement (UE) n° 910/2014 du 23 juillet 2014 précité ;

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

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

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

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'ANSSI.

V. **–** La commission des sanctions peut, en dernier recours, si le manquement persiste après que l’amende administrative prévue au I ou au II du présent article a été prononcée, 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.

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

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

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

~~Chapitre IV - dispositions diverses d'adaptation~~

##### #PJL#Résilience#article#38# [supprimé Sénat] [cryptologie]

~~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 État membre de l’Union européenne, l’importation et l’exportation des moyens de cryptologie assurant exclusivement des fonctions d’authentification ou de contrôle d’intégrité sont libres.~~

~~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~~.

##### #PJL#Résilience#article#39# [supprimé Sénat]

~~I. – Le chapitre Ier 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 … résilience» ;~~

~~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 [CPCE] 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 Ier de la loi n° 2018-133 du 26 février 2018 portant diverses dispositions d’adaptation au droit de l’Union européenne dans le domaine de la sécurité 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.~~

##### #PJL#Résilience#article#40# [supprimé Sénat]

[Article relatif aux Îles Wallis et Futuna, Polynésie française, Nouvelle-Calédonie]

~~Chapitre V - dispositions relatives aux communications électroniques~~

##### #PJL#Résilience#article#41# [supprimé Sénat]

~~L’article L. 39-1 du [CPCE] 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.~~

##### #PJL#Résilience#article#42# [supprimé Sénat]

~~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’État étrangères à l’impôt et au domaine.~~

~~Les décisions du ministre chargé des communications électroniques sont motivées et notifiées à l’intéressé. Elles peuvent être rendues publiques dans les publications, journaux ou services de communication au public par voie électronique choisis par lui, dans un format et pour une durée 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’État 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.~~

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* [end of document] \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*