N° 105

SÉNAT

SESSION ORDINAIRE DE 2017-2018

Enregistré à la Présidence du Sénat le 22 novembre 2017

PROJET DE LOI

(PROCÉDURE ACCÉLÉRÉE)

portant **diverses dispositions** *d'***adaptation** *au* **droit** *de l'***Union européenne** *dans le* **domaine** *de la* **sécurité**,

PRÉSENTÉ

au nom de M. Édouard PHILIPPE,

Premier ministre

Par M. Gérard COLLOMB,

ministre d'État, ministre de l'intérieur

(Envoyé à la commission des lois constitutionnelles, de législation, du suffrage universel, du Règlement et d'administration générale, sous réserve de la constitution éventuelle d'une commission spéciale dans les conditions prévues par le Règlement.)

EXPOSÉ DES MOTIFS

Mesdames, Messieurs,

Le projet de loi portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité a pour objet de transposer deux directives : la directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union (Titre I^{er}) et la directive (UE) 2017/853 du Parlement européen et du Conseil du 17 mai 2017 modifiant la directive 91/477/CEE du Conseil relative au contrôle de l'acquisition et de la détention d'armes (Titre II).

Ce projet de loi permet par ailleurs de tirer les conséquences de la décision n° 1104/2011/UE, en instaurant un mécanisme de sanction pour tout manquement aux obligations de protection du service public réglementé offert par le système mondial de radionavigation par satellite issu du programme GALILEO (Titre III).

TITRE I^{ER}

TRANSPOSITION DE LA DIRECTIVE 2016/1148

Le titre I^{er}, qui transpose dans le droit français la directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union, instaure de nouvelles obligations en matière de cyber-sécurité pour les opérateurs de services essentiels au fonctionnement de l'économie et de la société et les fournisseurs de services numériques.

Le premier chapitre regroupe les dispositions communes à l'ensemble de ce titre. L'**article 1er** définit les notions de « réseaux et systèmes d'information » et de « sécurité des réseaux et systèmes d'information ».

L'**article 2** précise le champ d'application du titre I^{er} et son articulation avec d'autres régimes visant à garantir la sécurité des systèmes d'information. Il reprend, d'une part, les deux catégories d'exclusions communes prévues par la directive et précise, d'autre part, que les

dispositions de ce titre ne sont pas applicables aux réseaux et systèmes d'informations soumis, en application d'actes sectoriels du droit de l'Union européenne, à des exigences en matière de sécurité et de notification d'incidents d'effet au moins équivalent.

L'**article 3** impose aux prestataires de services habilités à effectuer des contrôles en application du titre I^{er}, les mêmes obligations de confidentialité que celles applicables aux services de l'État. Il exige également la préservation des intérêts économiques des opérateurs de service essentiel et fournisseurs de services numériques lors de l'information du public par l'État des éventuels incidents de sécurité.

L'**article 4** renvoie à un décret en Conseil d'État la définition des modalités d'application du titre I^{er} et l'établissement de la liste des services essentiels au fonctionnement de la société ou de l'économie, qui déterminera le champ d'application du dispositif pour les opérateurs fournissant de tels services.

Le Chapitre II est consacré à la sécurité des réseaux et systèmes d'information des opérateurs de service essentiel au fonctionnement de la société ou de l'économie. **L'article 5** définit la notion d'opérateurs de service essentiels. Il confie au Premier ministre la responsabilité de désigner ces opérateurs et d'en actualiser la liste à intervalles réguliers. Il précise également que les systèmes d'information des opérateurs d'importance vitale mentionnés à l'article L. 1332-6-1 du code de la défense ne sont pas soumis aux dispositions de ce chapitre.

L'**article 6** confie au Premier ministre le soin d'édicter les règles de sécurité nécessaires à la protection de ces réseaux et systèmes d'information et prévoit que les opérateurs de services essentiels seront tenus d'appliquer ces règles à leurs frais.

L'**article 7** impose aux opérateurs de services essentiels de déclarer leurs incidents de sécurité à l'autorité nationale de sécurité des systèmes d'information. Il permet par ailleurs, en tant que de besoin, à l'autorité compétente de rendre publiques les informations ainsi recueillies et de les communiquer aux autorités d'autres États membres concernés par l'incident.

L'**article 8** prévoit la possibilité de soumettre ces opérateurs à des contrôles sur pièce et sur place par l'autorité nationale de sécurité des systèmes d'information ou des prestataires de services habilités à cet effet. Les opérateurs devront, le cas échéant, corriger tout manquement constaté lors de ces contrôles dans le délai imparti par une mise en demeure.

L'**article 9** parachève ce chapitre en instaurant des dispositions pénales pour sanctionner le non-respect des obligations ainsi fixées.

Le chapitre III est relatif au régime de sécurité applicable aux réseaux et systèmes d'information des fournisseurs de services numériques. L'**article 10** définit les notions de service numérique et de fournisseur de service numérique.

L'**article 11** définit quant à lui le champ d'application de ce régime conformément aux termes de la directive et reprend en particulier l'exclusion des microentreprises et petites entreprises dont il précise les seuils.

L'**article 12** impose à ces fournisseurs d'identifier les risques auxquels est exposée la sécurité de leurs réseaux et systèmes d'information et de prendre les mesures utiles pour gérer ces risques, éviter les incidents de nature à porter atteinte à la sécurité de leurs réseaux et systèmes d'information et en réduire l'impact.

L'**article 13** leur impose également une obligation de déclaration d'incident auprès de l'autorité nationale de sécurité des systèmes d'information dès lors qu'ils ont connaissance du caractère significatif de cet incident. Ces informations pourront être rendues publiques et communiquées en tant que de besoin aux autorités d'autres États membres concernés par l'incident. Cet article prévoit encore lorsque cela est nécessaire la mise en place d'une coopération avec les autorités des autres États membres concernés.

L'**article 14** prévoit la possibilité pour le Premier ministre de soumettre un fournisseur qui aurait méconnu l'une de ses obligations, à des contrôles sur place et sur pièce qui s'effectueront à ses frais. Ces fournisseurs devront, le cas échéant, corriger tout manquement constaté lors de ces contrôles à l'expiration du délai imparti par une mise en demeure.

Enfin, **l'article 15** clôture ce chapitre III en instaurant des sanctions pénales en cas de non-respect par les dirigeants de ces entreprises des obligations ainsi fixées.

TITRE II

TRANSPOSITION DE LA DIRECTIVE 2017/853

La grande majorité des dispositions prévues par la directive 2017/853 relève du domaine réglementaire. Des adaptations de la législation nationale sont néanmoins nécessaires.

La transposition de cette directive conduit à cet égard à modifier ou inscrire plusieurs dispositions dans la partie législative du code de la sécurité intérieure et du code de la défense. Elle ne retient que les mesures indispensables à cette transposition, exerçant, là où cela est nécessaire, le choix entre des options de transposition ouvertes aux États membres.

La directive du 18 juin 1991 avait été conçue initialement pour harmoniser le marché intérieur des armes civiles. La nouvelle directive modificative du 17 mai 2017, s'inscrit quant à elle, dans le prolongement de la directive 2008/51/CE du Parlement européen et du Conseil du 21 mai 2008, dans une logique de renforcement des mesures de sécurité.

La directive du 17 mai 2017, publiée au *Journal officiel de l'Union européenne* le 24 mai 2017, est entrée en vigueur le 13 juin 2017. La quasi-totalité de ses dispositions doit être transposée en droit national avant le 14 septembre 2018, conformément à son article 2.

L'**article 16** tire les conséquences de la suppression de la catégorie D des armes à feu, mentionnée dans la partie II de l'annexe I de la directive du 18 juin 1991 modifiée par la directive du 17 mai 2017. Il s'agit, en droit interne, des armes classées en catégorie D (1°), c'est-à-dire les armes soumises à enregistrement.

Ces armes de catégorie D soumises à enregistrement étant mentionnées à plusieurs reprises dans la loi, celle-ci doit être modifiée, pour tirer les conséquences de la disparition de cette catégorie.

La directive du 17 mai 2017 n'associe plus les reproductions d'armes historiques aux armes anciennes. Elle invite à prendre en considération les techniques modernes susceptibles d'améliorer la durabilité et la précision de ces reproductions d'armes historiques. En conséquence, le classement, opéré par la loi, de ces armes en catégorie D ne peut plus être systématique. Celles-ci feront l'objet d'un classement réglementaire en fonction de leurs caractéristiques techniques.

L'**article 17** tire les conséquences de la suppression de la catégorie D mentionnée à l'article 16 du présent projet de loi et prend par ailleurs en

compte le surclassement opéré par la directive de certaines armes à feu semi-automatiques - classées en droit interne en catégorie B (soumise à autorisation) - en catégorie A (interdite à l'acquisition et à la détention par les particuliers).

Des dérogations sont toutefois rendues possibles par la directive, au bénéfice de certaines catégories de détenteurs : les tireurs sportifs, certains services de sécurité privée et les collectionneurs d'armes. Le choix a été fait de limiter aux seuls tireurs sportifs et à certains services de sécurité privée, la possibilité de détenir ces armes nouvellement classées en catégorie A. Un décret en Conseil d'État précisera le champ de ces dérogations.

L'**article 18** modifie l'article L. 313-2 du code de la sécurité intérieure afin de tirer les conséquences de la directive du 17 mai 2017 laquelle soumet l'ensemble des professionnels à un contrôle portant sur leur honorabilité et leurs compétences professionnelles. Ce sont principalement les courtiers d'armes de catégorie C qui sont concernés, la loi ne prévoyant, pour eux, aucun contrôle d'honorabilité ni de compétence professionnelle. La transposition de la directive nécessite donc de soumettre cette profession à un contrôle administratif.

Le droit national généralise la possibilité de livraison au domicile de l'acquéreur des armes de toutes catégories, achetées à distance, sans garantie de contrôle effectif de l'identité de l'acquéreur et de son titre de détention. Cette dernière possibilité est supprimée, s'agissant des ventes entre particuliers, pour respecter les termes de la directive, selon laquelle les États membres veillent à ce que, dans le cadre, d'une vente à distance, l'identité et l'autorisation d'acquisition de l'acheteur fassent l'objet d'une vérification avant la livraison ou, au plus tard, lors de la livraison. Cette dernière exigence n'est effective, en droit interne, que pour les ventes réalisées par les professionnels : la dérogation à l'interdiction de livraison à domicile est donc supprimée s'agissant des ventes entre particuliers.

Enfin, les armuriers et les courtiers pourront refuser de conclure des transactions visant à acquérir des armes, des munitions ou leurs éléments qu'ils peuvent raisonnablement considérer comme suspectes. Ils devront signaler de telles transactions aux autorités de l'État.

Les **articles 19** et **20** tirent les conséquences de la suppression de la catégorie D mentionnée dans la partie II de l'annexe I de la directive du 18 juin 1991 modifiée, ainsi que du surclassement de certaines armes qui étaient auparavant classées en catégorie B.

L'**article 21** modifie le code de la défense afin de tirer les conséquences de la disparition de la catégorie D dans ce code.

TITRE III

MISE EN ŒUVRE DE LA DÉCISION N°1104/2011/UE

Le titre III transpose en droit français les obligations prévues par la décision n° 1104/2011/UE du Parlement européen et du Conseil du 25 octobre 2011 relative aux modalités d'accès au service public réglementé offert par le système mondial de radionavigation par satellite issu du programme Galileo. Le service public réglementé (SPR) de Galileo est un service réservé aux utilisateurs autorisés par les gouvernements, pour les applications sensibles qui exigent un contrôle d'accès efficace et un niveau élevé de continuité du service.

L'**article 22** introduit dans le code de la défense un chapitre relatif au service public réglementé de radionavigation par satellite issu du programme européen Galileo qui définit les activités liées à ce service qui font l'objet d'un contrôle par l'autorité administrative et instaure un régime de sanctions en cas de manquement aux obligations fixées par ces nouvelles dispositions.

L'article L. 2323-1 soumet à un régime d'autorisation l'accès au service public réglementé, le développement ou la fabrication de récepteurs ou de modules de sécurité conçus pour ce service et l'exportation d'équipements, de technologie ou de logiciels conçus pour ce service et prévoit les cas dans lesquels l'autorisation, qui peut être assortie de conditions ou de restrictions, peut être abrogée, retirée, modifiée ou suspendue. Afin de permettre à l'autorité administrative de vérifier que les destinataires d'équipements, de technologie ou de logiciels concernés sont eux-mêmes autorisés à accéder au service public réglementé, l'article L. 2323-2 met en place un régime de déclaration pour les transferts effectués depuis la France vers les autres États membres de l'Union européenne.

L'article L. 2323-3 renvoie à un décret en Conseil d'État la définition des modalités d'application des régimes d'autorisation et de déclaration ainsi créés. Il précise, en outre, l'articulation de ce dispositif avec les dispositions du code de la défense applicables aux importations, exportations et transferts des matériels de guerre et assimilés et celles du règlement n° 428/2009 du Conseil du 5 mai 2009 instituant un régime communautaire de contrôle des exportations, des transferts, du courtage et du transit de biens à double usage.

Les articles L. 2323-4 à L. 2323-6 définissent les sanctions pénales encourues en cas de manquement aux obligations définies par ce nouveau chapitre ou de tentative de commission de ces infractions, qui pourront être assorties de peines complémentaires, tant pour les personnes physiques que pour les personnes morales.

TITRE IV

DISPOSITIONS APPLICABLES À L'OUTRE-MER

L'**article 23** rend la loi applicable sur l'ensemble du territoire de la République en procédant aux modifications nécessaires des articles du code de la sécurité intérieure et du code de la défense suivant la technique du « compteur Lifou ».

Par ailleurs, pour les collectivités régies par le principe de spécialité législative, cet article prévoit les grilles de lecture nécessaires pour l'application des dispositions comportant des références au droit communautaire.

TITRE V

DISPOSITIONS TRANSITOIRES

L'**article 24** introduit des dispositions relatives à l'entrée en vigueur des différents articles des chapitres I^{er} et III du titre I et du titre II afin de gérer la période transitoire entre le vote de la loi et la publication de ses décrets d'application. Le projet de loi précise que leur entrée en vigueur interviendra, selon les cas, aux dates que prévoiront ces décrets, et au plus tard aux dates limites de transposition fixée par chaque directive.

PROJET DE LOI

Le Premier ministre,

Sur le rapport du ministre d'État, ministre de l'intérieur,

Vu l'article 39 de la Constitution,

Décrète :

Le présent projet de loi portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité, délibéré en Conseil des ministres après avis du Conseil d'État, sera présenté au Sénat par le ministre d'État, ministre de l'intérieur, qui sera chargé d'en exposer les motifs et d'en soutenir la discussion.

TITRE I^ER

DISPOSITIONS TENDANT A TRANSPOSER LA DIRECTIVE (UE) 2016/1148 DU PARLEMENT EUROPEEN ET DU CONSEIL DU 6 JUILLET 2016 CONCERNANT DES MESURES DESTINEES A ASSURER UN NIVEAU ELEVE COMMUN DE SECURITE DES RESEAUX ET DES SYSTEMES D'INFORMATION DANS L'UNION

CHAPITRE I^ER

Dispositions communes

Article 1er

① Pour l'application du présent titre, on entend par réseau et système d'information :

② 1° Tout réseau de communication électronique tel que défini au 2° de l'article L. 32 du code des postes et des communications électroniques ;

③ 2° Tout dispositif ou tout ensemble de dispositifs interconnectés ou apparentés, dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement automatisé de données numériques ;

④ 3° Les données numériques stockées, traitées, récupérées ou transmises par les éléments mentionnés aux 1° et 2° en vue de leur fonctionnement, utilisation, protection et maintenance.

⑤ La sécurité des réseaux et systèmes d'information consiste en leur capacité de résister, à un niveau de confiance donné, à des actions qui compromettent la disponibilité, l'authenticité, l'intégrité ou la confidentialité de données stockées, transmises ou faisant l'objet d'un traitement, et des services connexes que ces réseaux et systèmes d'information offrent ou rendent accessibles.

Article 2

① Les dispositions du présent titre ne sont pas applicables aux entreprises exploitant des réseaux de communications électroniques ouverts au public ou fournissant des services de communications électroniques accessibles au public ni aux prestataires de services de confiance soumis aux exigences énoncées à l'article 19 du règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE.

② Elles ne sont pas non plus applicables aux réseaux et systèmes d'information des opérateurs de services essentiels et des fournisseurs de service numérique lorsque ces réseaux et systèmes d'information sont soumis, en application d'un acte juridique de l'Union européenne, à des exigences sectorielles de sécurité ou de notification des incidents ayant un effet au moins équivalent aux obligations résultant de l'application des dispositions du présent titre.

Article 3

① Les prestataires de service habilités à effectuer des contrôles en application du présent titre sont soumis aux mêmes règles de confidentialité que les services de l'État à l'égard des informations qu'ils recueillent auprès des opérateurs mentionnés à l'article 5 et des fournisseurs de service numérique mentionnés à l'article 11.

② Lorsqu'il informe le public ou les Etats membres de l'Union européenne d'incidents dans les conditions prévues aux articles 7 et 13, l'État tient compte des intérêts économiques de ces opérateurs et fournisseurs de service numérique et veille à ne pas révéler d'informations susceptibles de porter atteinte à leur sécurité et au secret en matière commerciale et industrielle.

Article 4

Les modalités d'application du présent titre sont déterminées par décret en Conseil d'État. Ce décret fixe notamment la liste des services essentiels au fonctionnement de la société ou de l'économie mentionnés à l'article 5.

CHAPITRE II

Dispositions relatives à la sécurité des reseaux et systèmes d'information des opérateurs de services essentiels

Article 5

① Les opérateurs, publics ou privés, offrant des services essentiels au fonctionnement de la société ou de l'économie et qui pourraient être gravement perturbés par des incidents affectant les réseaux et systèmes d'information nécessaires à la fourniture de ces services sont soumis aux dispositions du présent chapitre pour la sécurité de ces réseaux et systèmes d'information. Ces opérateurs sont désignés par le Premier ministre au regard des services qu'ils fournissent et des conséquences qu'auraient de tels incidents sur leurs services. La liste de ces opérateurs est actualisée à intervalles réguliers et au moins tous les deux ans.

② Les dispositions du présent chapitre ne sont pas applicables aux systèmes d'information mentionnés au premier alinéa de l'article L. 1332-6-1 du code de la défense.

Article 6

① Le Premier ministre fixe les règles de sécurité nécessaires à la protection des réseaux et systèmes d'information mentionnés au premier alinéa de l'article 5. Ces règles ont pour objet de garantir un niveau de sécurité adapté au risque existant, compte tenu de l'état des connaissances. Elles définissent les mesures appropriées pour prévenir les incidents qui compromettent la sécurité des réseaux et systèmes d'information utilisés pour la fourniture des services essentiels ou pour en limiter l'impact afin d'assurer la continuité de ces services essentiels. Les opérateurs mentionnés au même article appliquent ces règles à leurs frais.

② Les règles prévues au premier alinéa peuvent notamment prescrire que les opérateurs recourent à des dispositifs matériels ou logiciels ou à des services informatiques dont la sécurité a été certifiée.

Article 7

① Les opérateurs mentionnés à l'article 5 déclarent, sans retard injustifié, à l'autorité nationale de sécurité des systèmes d'information mentionnée à l'article L. 2321-1 du code de la défense, les incidents affectant les réseaux et systèmes d'information nécessaires à la fourniture de services essentiels, lorsque ces incidents ont ou sont susceptibles d'avoir, compte tenu notamment du nombre d'utilisateurs et de la zone géographique touchés ainsi que de la durée de l'incident, un impact significatif sur la continuité de ces services.

② Après avoir consulté l'opérateur concerné, le Premier ministre peut informer le public d'un incident mentionné au premier alinéa, lorsque cette information est nécessaire pour prévenir ou traiter un incident. En outre, lorsqu'un incident a un impact significatif sur la continuité de services essentiels fournis par l'opérateur à d'autres Etats membres de l'Union européenne, le Premier ministre en informe les autorités ou organismes compétents de ces Etats.

Article 8

① Le Premier ministre peut soumettre les opérateurs mentionnés à l'article 5 à des contrôles destinés à vérifier le respect des obligations prévues par le présent chapitre ainsi que le niveau de sécurité des réseaux et systèmes d'information nécessaires à la fourniture de services essentiels.

② Les contrôles sont effectués, sur pièce et sur place, par l'autorité nationale de sécurité des systèmes d'information mentionnée à l'article L. 2321-1 du code de la défense ou par des prestataires de service qualifiés. Le coût des contrôles est à la charge des opérateurs. La qualification de prestataire de service habilité à effectuer ces contrôles est délivrée par le Premier ministre.

③ Les opérateurs sont tenus de communiquer à l'autorité ou au prestataire de service chargé du contrôle prévu au premier alinéa les informations et éléments nécessaires pour réaliser le contrôle, y compris les documents relatifs à leur politique de sécurité et les résultats d'audit de sécurité et leur permettre d'accéder aux réseaux et systèmes d'information soumis au contrôle afin d'effectuer des analyses et des relevés d'informations techniques.

④ Ils corrigent tout manquement à leurs obligations qui aurait été ainsi constaté dans le délai imparti par la mise en demeure notifiée à l'issue du contrôle.

Article 9

① Est puni d'une amende de 100 000 € le fait, pour les dirigeants des opérateurs mentionnés à l'article 5, de ne pas se conformer aux règles de sécurité mentionnées à l'article 6 et rappelées dans une mise en demeure, à l'expiration du délai défini par celle-ci.

② Est puni d'une amende de 75 000 € le fait, pour les mêmes personnes, de ne pas satisfaire à l'obligation de déclaration d'incident prévue au premier alinéa de l'article 7.

③ Est puni d'une amende de 125 000 € le fait, pour les mêmes personnes, de faire obstacle aux opérations de contrôle mentionnées à l'article 8.

CHAPITRE III

Dispositions relatives à la sécurité des reseaux et systèmes d'information des fournisseurs de service numérique

Article 10

① Pour l'application du présent chapitre, on entend :

② 1° Par service numérique tout service fourni normalement contre rémunération, à distance, par voie électronique et à la demande individuelle d'un destinataire de services ;

③ 2° Par fournisseur de service numérique toute personne morale qui fournit l'un des services suivants :

④ *a)* Place de marché en ligne à savoir un service numérique qui permet à des consommateurs ou à des professionnels au sens du *a* de l'article L. 151-1 du code de la consommation de conclure des contrats de vente ou de service en ligne avec des professionnels soit sur le site internet de la place de marché en ligne, soit sur le site internet d'un professionnel qui utilise les services informatiques fournis par la place de marché en ligne ;

⑤ *b)* Moteurs de recherche en ligne à savoir un service numérique qui permet aux utilisateurs d'effectuer des recherches sur, en principe, tous les sites internet ou sur les sites internet dans une langue donnée, sur la base d'une requête lancée sur n'importe quel sujet sous la forme d'un mot clé, d'une phrase ou d'une autre entrée, et qui renvoie des liens à partir desquels il est possible de trouver des informations en rapport avec le contenu demandé ;

⑥ *c)* Service d'informatique en nuage à savoir un service numérique qui permet l'accès à un ensemble modulable et variable de ressources informatiques pouvant être partagées.

Article 11

① Sont soumis aux dispositions du présent chapitre les fournisseurs de service numérique qui offrent leurs services dans l'Union européenne et qui soit ont leur siège social sur le territoire national, soit, n'étant pas établis dans l'Union européenne, ont désigné à cet effet un représentant sur le territoire national.

② Les dispositions du présent chapitre ne sont pas applicables aux entreprises qui emploient moins de cinquante salariés et dont le chiffre d'affaires annuel n'excède pas 10 millions d'euros.

Article 12

① Les fournisseurs de service numérique mentionnés à l'article 11 garantissent, compte tenu de l'état des connaissances, un niveau de sécurité des réseaux et des systèmes d'information nécessaires à la fourniture de leurs services dans l'Union européenne adapté aux risques existants. A cet effet, ils identifient les risques qui menacent la sécurité de ces réseaux et systèmes d'information et prennent les mesures techniques et organisationnelles nécessaires et proportionnées pour gérer ces risques. Ces mesures prennent notamment en considération la sécurité des systèmes et des installations, la gestion des incidents, la gestion de la continuité des activités, le suivi, l'audit et le contrôle ainsi que le respect des normes internationales.

② Les fournisseurs de service numérique prennent en outre les mesures utiles destinées, d'une part, à éviter les incidents de nature à porter atteinte à la sécurité des réseaux et systèmes d'information nécessaires à la fourniture de leurs services dans l'Union européenne et, d'autre part, à en réduire au minimum l'impact, de manière à garantir la continuité de ces services.

Article 13

① Les fournisseurs de service numérique mentionnés à l'article 11 déclarent, sans retard injustifié, à l'autorité nationale de sécurité des systèmes d'information mentionnée à l'article L. 2321-1 du code de la défense, les incidents affectant les réseaux et systèmes d'information nécessaires à la fourniture de leurs services dans l'Union européenne, lorsque les informations dont ils disposent font apparaître que ces incidents ont un impact significatif sur la fourniture de ces services, compte tenu notamment du nombre d'utilisateurs touchés par l'incident, de sa durée, de sa portée géographique, de la gravité de la perturbation du fonctionnement du service et de son impact sur le fonctionnement de la société ou de l'économie.

② Après avoir consulté le fournisseur de service numérique concerné, le Premier ministre peut informer le public d'un incident mentionné au premier alinéa ou imposer au fournisseur de le faire, lorsque cette information est nécessaire pour prévenir ou traiter un incident ou est justifiée par un motif d'intérêt général. En outre, lorsqu'un incident a des conséquences significatives sur les services fournis à d'autres Etats membres de l'Union européenne, le Premier ministre en informe les autorités ou organismes compétents de ces Etats, qui peuvent rendre public l'incident.

Article 14

① Lorsque le Premier ministre est informé qu'un fournisseur de service numérique mentionné à l'article 11 ne satisfait pas à l'une des obligations prévues aux articles 12 ou 13, il peut le soumettre à des contrôles destinés à vérifier le respect des obligations prévues par le présent chapitre ainsi que le niveau de sécurité des réseaux et systèmes d'information nécessaires à la fourniture de ces services. Il en informe si nécessaire les autorités compétentes des autres Etats membres dans lesquels sont situés des réseaux et systèmes d'information de ce fournisseur et coopère avec elles.

② Les contrôles sont effectués, sur pièce et sur place, par l'autorité nationale de sécurité des systèmes d'information mentionnée à l'article L. 2321-1 du code de la défense ou par des prestataires de service qualifiés. Le coût des contrôles est à la charge des fournisseurs de service numérique. La qualification de prestataire de service habilité à effectuer ces contrôles est délivrée par le Premier ministre.

③ Les fournisseurs de service numérique sont tenus de communiquer à l'autorité ou au prestataire de service chargé du contrôle prévu au premier alinéa les informations nécessaires pour évaluer la sécurité de leurs réseaux et systèmes d'information, y compris les documents relatifs à leurs politiques de sécurité et leur permettre d'accéder aux réseaux et systèmes d'information soumis au contrôle afin d'effectuer des analyses et des relevés d'informations techniques.

④ Ils corrigent tout manquement à leurs obligations qui aurait été ainsi constaté dans le délai imparti par la mise en demeure notifiée à l'issue du contrôle.

Article 15

① Est puni d'une amende de 75 000 € le fait, pour les dirigeants des fournisseurs de service numérique mentionnés à l'article 11, de ne pas prendre les mesures de sécurité nécessaires conformément aux dispositions de l'article 12 et mentionnées dans une mise en demeure, à l'expiration du délai défini par celle-ci.

② Est puni d'une amende de 50 000 € le fait, pour les mêmes personnes, de ne pas satisfaire aux obligations de déclaration d'incident ou d'information du public prévues à l'article 13.

③ Est puni d'une amende de 100 000 € le fait, pour les mêmes personnes, de faire obstacle aux opérations de contrôle mentionnées à l'article 14.

TITRE II

DISPOSITIONS RELATIVES AU CONTROLE DE L'ACQUISITION ET DE LA DETENTION D'ARMES

Article 16

① Le chapitre I^{er} du titre I^{er} du livre III du code de la sécurité intérieure est ainsi modifié :

② 1° L'article L. 311-2 est ainsi modifié :

③ *a)* Au 4°, les mots : « soumises à enregistrement et armes » sont supprimés ;

④ *b)* A la seconde phrase du neuvième alinéa, les mots : « ou des enregistrements » sont supprimés ;

⑤ 2° A l'article L. 311-4, les mots : « en catégorie D » sont remplacés par les mots : « par décret en Conseil d'État ».

Article 17

① Le chapitre II du titre I[er] du livre III du même code est ainsi modifié :

② 1° A la dernière phrase de l'article L. 312-2, après les mots : « matériels de guerre », sont insérés les mots : « , armes et éléments d'armes de catégorie A », et les mots : « à fin de collection, professionnelle ou sportive par des personnes » sont remplacés par les mots : « , pour des activités sportives, professionnelles ou de collection » ;

③ 2° L'article L. 312-3 est ainsi modifié :

④ *a)* Au premier alinéa, les mots : « B et C et d'armes de catégorie D soumises à enregistrement » sont remplacés par les mots : « A, B et C » ;

⑤ *b)* Au quarante-deuxième alinéa du 1°, les mots : « ou enregistrement » et les mots : « ou d'armes de catégorie D » sont supprimés ;

⑥ *c)* Au quarante-cinquième alinéa du 1°, les mots : « ou d'armes de catégorie D soumises à enregistrement » sont supprimés ;

⑦ 3° A l'article L. 312-3-1, les mots : « B et C et des armes de catégorie D soumises à enregistrement » sont remplacés par les mots : « A, B et C » ;

⑧ 4° A la première phrase du premier alinéa et aux deuxième et troisième alinéas de l'article L. 312-4, avant la lettre : « B » sont insérés les mots : « A ou » ;

⑨ 5° L'article L. 312-4-2 est abrogé ;

⑩ 6° Aux 1° et 2° de l'article L. 312-4-3, avant la lettre : « B » sont insérés les mots : « A ou » ;

⑪ 7° A l'article L. 312-5, les mots : « D figurant sur une liste établie par un décret en Conseil d'État » sont remplacés par la lettre : « C » ;

⑫ 8° L'article L. 312-11 est ainsi modifié :

⑬ *a)* Au premier alinéa, les mots : « des catégories B, C et D » sont remplacés par les mots : « de toute catégorie » ;

⑭ *b)* Au deuxième alinéa, les mots : « soit à la neutraliser, » sont supprimés ;

⑮ 9° Au premier alinéa de l'article L. 312-13, les mots : « des catégories B, C et D » sont remplacés par les mots : « de toute catégorie » ;

⑯ 10° Aux 2° et 3° de l'article L. 312-16, les mots : « B et C et des armes de catégorie D soumises à enregistrement » sont remplacés par les mots : « A, B et C ».

Article 18

① Le chapitre III du titre I^er^ du livre III du même code est ainsi modifié :

② 1° L'article L. 313-2 est ainsi modifié :

③ *a)* Au premier alinéa, après les mots : « le commerce, » sont insérés les mots : « l'intermédiation, » et après les mots : « la location, » sont insérés les mots : « la location-vente, le prêt, la modification, » ;

④ *b)* Le second alinéa est supprimé ;

⑤ 2° Le dernier alinéa de l'article L. 313-3 est supprimé ;

⑥ 3° L'article L. 313-5 est remplacé par les dispositions suivantes :

⑦ « *Art. L. 313-5.* – Sauf si la transaction a été faite dans le cadre des activités mentionnées à l'article L. 313-2, les matériels, armes ou leurs éléments essentiels des catégories A, B, C ainsi que des armes de catégorie D énumérées par décret en Conseil d'État, qui, par dérogation aux dispositions du premier alinéa de l'article L. 313-4, sont acquis par correspondance, à distance ou directement entre particuliers ne peuvent être livrés que dans les locaux mentionnés aux premier et troisième alinéas de l'article L. 313-3, aux fins de vérification de l'identité de l'acquéreur, des pièces mentionnées à l'article L. 312-4-1 ou, le cas échéant, de l'autorisation d'acquisition et de détention de l'acquéreur mentionnée à l'article L. 312-4.

⑧ « La transaction est réputée parfaite à compter de la remise effective à l'acquéreur.

⑨ 4° Après l'article L. 313-5, sont insérés deux articles L. 313-6 et L. 313-7 ainsi rédigés :

⑩ « *Art. L. 313-6.* – Les armuriers et les courtiers mentionnés à l'article L. 313-2 peuvent refuser de conclure toute transaction visant à acquérir des armes, des munitions ou leurs éléments dont il est raisonnable de considérer qu'elle présente un caractère suspect.

⑪ « Toute tentative de transaction suspecte fait l'objet d'un signalement auprès d'un service désigné par le ministre de l'intérieur.

⑫ « *Art. L. 313-7.* – Un décret en Conseil d'État précise les modalités d'application du présent chapitre. ».

Article 19

① I. – A l'article L. 314-2-1 du même code, les mots : « ou de catégorie D soumises à enregistrement » et les mots : « ou, le cas échéant, à un enregistrement » sont supprimés.

② II. – A l'article L. 315-1 du même code, après la lettre : « B » sont insérés les mots : « et C » et les mots : « des catégories A et B » sont remplacés par les mots : « de ces mêmes catégories ».

Article 20

① Le chapitre VII du titre I^{er} du livre III du même code est ainsi modifié :

② 1° Au premier alinéa de l'article L. 317-3-1, les mots : « , C ainsi que d'une ou plusieurs armes ou munitions de catégorie D mentionnées au second alinéa de l'article L. 312-4-2 » sont remplacés par les mots : « et C » ;

③ 2° Au 4° de l'article L. 317-3-2, les mots : « ou une arme, un élément essentiel ou des munitions de catégorie D mentionnés au second alinéa de l'article L. 312-4-1, » sont supprimés ;

④ 3° Le deuxième alinéa de l'article L. 317-4-1 est supprimé.

Article 21

① Le titre III du livre III de la deuxième partie du code de la défense est ainsi modifié :

② 1° L'article L. 2331-1 est ainsi modifié :

③ *a)* Au 4° du I, les mots : « armes soumises à enregistrement et » sont supprimés ;

④ *b)* Au neuvième alinéa du I, les mots : « ou des enregistrements » sont supprimés ;

⑤ *c)* Au III, après les mots : « du présent titre » sont insérés les mots : « ou au chapitre III du titre I[er] du livre III du code de la sécurité intérieure » ;

⑥ 2° Au premier alinéa de l'article L. 2339-4, les mots : « , C ainsi que d'une ou plusieurs armes ou munitions de catégorie D mentionnées au second alinéa de l'article L. 312-4-2 du code de la sécurité intérieure » sont remplacés par les mots : « et C » ;

⑦ 3° Au 4° de l'article L. 2339-4-1, les mots : « ou une arme, un élément essentiel ou des munitions de catégorie D mentionnés au second alinéa de l'article L. 312-4-2 du code de la sécurité intérieure » sont supprimés.

TITRE III

DISPOSITIONS RELATIVES AU SERVICE PUBLIC REGLEMENTE GALILEO

Article 22

① Le titre II du livre III de la deuxième partie du code de la défense est complété par un chapitre ainsi rédigé :

② *« CHAPITRE III*

③ ***« Service public réglementé de radionavigation par satellite***

④ *« Section 1*

⑤ ***« Activités contrôlées***

⑥ « *Art. L. 2323-1*. – L'accès au service public réglementé offert par le système mondial de radionavigation par satellite issu du programme européen Galileo, le développement ou la fabrication de récepteurs ou de modules de sécurité conçus pour ce service et l'exportation d'équipements, de technologie ou de logiciels conçus pour ce service ne peuvent s'exercer qu'après autorisation délivrée par l'autorité administrative et sous son contrôle.

⑦ « Les autorisations délivrées en application du présent article peuvent être assorties de conditions ou de restrictions. Elles peuvent être abrogées, retirées, modifiées ou suspendues en cas de manquement du titulaire aux conditions spécifiées dans l'autorisation ou lorsque le respect des engagements internationaux de la France, la protection du service public réglementé ou celle des intérêts essentiels d'ordre public ou de sécurité publique le justifient.

⑧ « *Art. L. 2323-2*. – Tout transfert d'équipements, de technologie ou de logiciels conçus pour le service public réglementé offert par le système mondial de radionavigation par satellite issu du programme européen Galileo effectué depuis la France vers les autres Etats membres de l'Union européenne fait l'objet d'une déclaration à l'autorité administrative.

⑨ « *Art. L. 2323-3*. – Les dispositions de la présente section s'appliquent sans préjudice de celles du chapitre V du titre III du présent livre et du règlement n° 428/2009 du Conseil du 5 mai 2009 instituant un régime communautaire de contrôle des exportations, des transferts, du courtage et du transit de biens à double usage.

⑩ « Les modalités d'application de la présente section sont fixées par décret en Conseil d'État.

⑪ *« Section 2*

⑫ ***« Sanctions pénales***

⑬ « *Art. L. 2323-4*. – Est puni d'une amende de 200 000 € le fait de se livrer à une activité définie à l'article L. 2323-1 :

⑭ « 1° Sans autorisation ;

⑮ « 2° Sans respecter les conditions ou restrictions dont est assortie l'autorisation mentionnée à l'article L. 2323-1.

⑯ « La tentative des délits prévus aux alinéas précédents est punie des mêmes peines.

⑰ « *Art. L. 2323-5*. – Est punie d'une amende de 50 000 € la méconnaissance de l'obligation prévue à l'article L. 2323-2.

⑱ « *Art. L. 2323-6*. – I. – Les personnes physiques coupables de l'une des infractions prévues aux articles L. 2323-4 et L. 2323-5 encourent également les peines complémentaires suivantes :

⑲ « 1° La confiscation, suivant les modalités prévues par l'article 131-21 du code pénal, de la chose qui a servi ou était destinée à commettre l'infraction ou de la chose qui en est le produit, à l'exception des objets susceptibles de restitution ;

⑳ « 2° L'interdiction, suivant les modalités prévues par l'article 131-27 du même code et pour une durée de cinq ans au plus, d'exercer une fonction publique ou d'exercer l'activité professionnelle ou sociale dans l'exercice ou à l'occasion de l'exercice de laquelle l'infraction a été commise ;

㉑ « 3° La fermeture, dans les conditions prévues par l'article 131-33 du même code et pour une durée de cinq ans au plus, des établissements ou de l'un ou de plusieurs des établissements de l'entreprise ayant servi à commettre les faits incriminés ;

㉒ « 4° L'exclusion, dans les conditions prévues par l'article 131-34 du même code et pour une durée de cinq ans au plus, des marchés publics.

㉓ « II. – Les personnes morales déclarées responsables pénalement, dans les conditions prévues par l'article 121-2 du code pénal, des infractions définies à la présente section encourent, outre l'amende suivant les modalités prévues par l'article 131-38 du même code, les peines prévues par les 1°, 2°, 4°, 5°, 8°, 9° et 12° de l'article 131-39 de ce code. »

TITRE IV

DISPOSITIONS APPLICABLES A L'OUTRE-MER

Article 23

① I. – Les dispositions des titres I^{er} et V s'appliquent sur l'ensemble du territoire de la République.

② Pour l'application du titre I^{er} à Wallis et Futuna, en Polynésie française, en Nouvelle-Calédonie et dans les Terres australes et antarctiques françaises, la référence au règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE est remplacée par la référence au droit applicable en métropole en vertu de ce règlement.

③ II. – Le titre IV du livre III du code de la sécurité intérieure est ainsi modifié :

④ 1° Aux articles L. 344-1, L. 345-1, L. 346-1 et L. 347-1, les mots : « de la loi n° 2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale » sont remplacés par les mots : « de la loi n° …… du ……. portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité » ;

⑤ 2° Au premier alinéa de l'article L. 345-2-1, les mots : « et du 1° de la catégorie D » sont supprimés.

⑥ III. – Le livre IV de la deuxième partie du code de la défense est ainsi modifié :

⑦ 1° Les articles L. 2441-1, L. 2451-1, L. 2461-1 et L. 2471-1 sont ainsi modifiés :

⑧ *a)* Au premier alinéa de chaque article, les références : « L. 2322-1 à L. 2335-7 » sont remplacées par les références : « L. 2322-1, L. 2323-1, L. 2323-3, L. 2323-4, L. 2323-6, L. 2331-1 à L. 2335-7 » ;

⑨ *b)* A chaque article, il est ajouté un alinéa ainsi rédigé :

⑩ « Les dispositions des articles L. 2323-1, L. 2323-3, L. 2323-4, L. 2323-6, L. 2331-1, L. 2339-4 et L. 2339-4-1 sont applicables dans leur rédaction issue de la loi n° ……» ;

⑪ 2° Au début de l'article L. 2441-3-1, il est inséré deux alinéas ainsi rédigés :

⑫ « Pour l'application à Wallis et Futuna des dispositions de l'article L. 2323-3, la référence au règlement n° 428/2009 du Conseil du 5 mai 2009 instituant un régime communautaire de contrôle des exportations, des transferts, du courtage et du transit de biens à double usage est remplacée par la référence au droit applicable en métropole en vertu de ce règlement.

⑬ « Pour l'application à Wallis et Futuna des dispositions de l'article L. 2323-6, la référence à l'article L. 2323-5 est supprimée. » ;

⑭ 3° Au début de l'article L. 2451-4-1, il est inséré deux alinéas ainsi rédigés :

⑮ « Pour l'application en Polynésie française des dispositions de l'article L. 2323-3, la référence au règlement n° 428/2009 du Conseil du 5 mai 2009 instituant un régime communautaire de contrôle des exportations, des transferts, du courtage et du transit de biens à double usage est remplacée par la référence au droit applicable en métropole en vertu de ce règlement.

⑯ « Pour l'application en Polynésie française des dispositions de l'article L. 2323-6, la référence à l'article L. 2323-5 est supprimée. » ;

⑰ 4° Au début de l'article L. 2461-4-1, il est inséré deux alinéas ainsi rédigés :

⑱ « Pour l'application en Nouvelle-Calédonie des dispositions de l'article L. 2323-3, la référence au règlement n° 428/2009 du Conseil du 5 mai 2009 instituant un régime communautaire de contrôle des exportations, des transferts, du courtage et du transit de biens à double usage est remplacée par la référence au droit applicable en métropole en vertu de ce règlement.

⑲ « Pour l'application en Nouvelle-Calédonie des dispositions de l'article L. 2323-6, la référence à l'article L. 2323-5 est supprimée. » ;

⑳ 5° Au début de l'article L. 2471-3-1, il est inséré deux alinéas ainsi rédigés :

㉑ « Pour l'application dans les Terres australes et antarctiques françaises des dispositions de l'article L. 2323-3, la référence au règlement n° 428/2009 du Conseil du 5 mai 2009 instituant un régime communautaire de contrôle des exportations, des transferts, du courtage et du transit de biens à double usage est remplacée par la référence au droit applicable en métropole en vertu de ce règlement.

㉒ « Pour l'application dans les Terres australes et antarctiques françaises des dispositions de l'article L. 2323-6, la référence à l'article L. 2323-5 est supprimée. »

TITRE V

DISPOSITIONS TRANSITOIRES

Article 24

① Les dispositions des chapitres I^er^ et III du titre I^er^ entrent en vigueur à compter d'une date définie par décret en Conseil d'État et au plus tard le 9 mai 2018. La désignation des opérateurs de services essentiels prévue au premier alinéa de l'article 5 intervient au plus tard le 9 novembre 2018.

② Les dispositions des articles 16, 17, 19, 20, 21 ainsi que des 2°, 3° et 4° de l'article 18 entrent en vigueur à compter d'une date définie par décret en Conseil d'État et au plus tard le 14 septembre 2018.

③ Les dispositions du 1° de l'article 18 entrent en vigueur à compter d'une date fixée par décret en Conseil d'État et au plus tard le 14 décembre 2019.

④ Les personnes qui, à la date d'entrée en vigueur de la présente loi, détiennent des armes acquises depuis le 13 juin 2017 qui étaient précédemment soumises à enregistrement au titre du 1° de la catégorie D et sont désormais soumises à déclaration au titre de leur classement dans la catégorie C, procèdent à leur déclaration auprès du représentant de l'État dans le département du lieu de leur domicile ou, à Paris, du préfet de police, dans les conditions fixées par décret en Conseil d'État et au plus tard le 14 décembre 2019.

Fait à Paris, le 22 novembre 2017

Signé : ÉDOUARD PHILIPPE

Par le Premier ministre :

Le ministre d'État, ministre de l'intérieur

Signé : GÉRARD COLLOMB

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

ÉTUDE D'IMPACT

PROJET DE LOI

PORTANT DIVERSES DISPOSITIONS D'ADAPTATION AU DROIT DE L'UNION EUROPÉENNE DANS LE DOMAINE DE LA SÉCURITÉ

NOR : INTX1728622L/Bleue-1

17 novembre 2017

INTRODUCTION GÉNÉRALE

Le projet de loi portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité a pour objet de transposer deux directives : la directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union et la directive (UE) 2017/853 du Parlement européen et du Conseil du 17 mai 2017 modifiant la directive 91/477/CEE du Conseil relative au contrôle de l'acquisition et de la détention d'armes.

Ce projet de loi a par ailleurs pour objet de tirer les conséquences de la décision n° 1104/2011/UE du Parlement européen et du Conseil du 25 octobre 2011, en instaurant un mécanisme de sanction pour tout manquement aux obligations de protection du service public réglementé offert par le système mondial de radionavigation par satellite issu du programme Galileo.

La transposition en droit interne des deux directives entend éviter toute « surtransposition ».

Le titre I, qui transpose dans le droit français la directive 2016/1148 du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union, instaure de nouvelles obligations en matière de cyber-sécurité pour les opérateurs de services essentiels au fonctionnement de l'économie et de la société et les fournisseurs de services numériques.

Le titre II transpose la directive 2017/853 du 17 mai 2017 modifiant la directive 91/477/CEE relative au contrôle de l'acquisition et de la détention d'armes, renforçant le contrôle du commerce et de la circulation des armes à feu « civiles ».

Le titre III transpose en droit français les obligations prévues par la décision n° 1104/2011/UE du 25 octobre 2011 relative aux modalités d'accès au service public réglementé offert par le système mondial de radionavigation par satellite issu du programme Galileo. Le service public réglementé (SPR) de Galileo est un service réservé aux utilisateurs autorisés par les gouvernements, pour les applications sensibles qui exigent un contrôle d'accès efficace et un niveau élevé de continuité du service.

TABLEAU SYNOPTIQUE DES TEXTES D'APPLICATION

ARTICLES	TEXTES D'APPLICATION	ADMINISTRATION COMPETENTE
1er	Décret en Conseil d'Etat	ANSSI
2	Décret en Conseil d'Etat Arrêté du Premier ministre	ANSSI
3	Décret en Conseil d'Etat	ANSSI
4	Décret en Conseil d'Etat Arrêté du Premier ministre	ANSSI
5	Décret en Conseil d'Etat	ANSSI
8	Décret en Conseil d'Etat	ANSSI
9	Décret en Conseil d'Etat	ANSSI
10	Décret en Conseil d'Etat Arrêté du Premier ministre	ANSSI
11	Décret en Conseil d'Etat	ANSSI
14	Décret en Conseil d'État	Ministère de l'intérieur Service central des armes
15	Décret en Conseil d'État	Ministère de l'intérieur Service central des armes
16	Décret en Conseil d'État	Ministère de l'intérieur Service central des armes
20	Décret en Conseil d'Etat	SGDSN

TABLEAU SYNOPTIQUE DES CONSULTATIONS MENÉES

ARTICLES	CONTENU	INSTANCE CONCERNÉE
2° du II de l'article 23	Suppression des mots : « et du 1° de la catégorie D » au premier alinéa de l'article L. 345-2-1 du code de la sécurité intérieure	Congrès de la Nouvelle-Calédonie (fondement : articles 89 et 90 de la loi organique n° 99-209)

TITRE I - TRANSPOSITION DE LA DIRECTIVE (UE) 2016/1148 DU PARLEMENT EUROPÉEN ET DU CONSEIL DU 6 JUILLET 2016 CONCERNANT DES MESURES DESTINÉES À ASSURER UN NIVEAU ÉLEVÉ COMMUN DE SÉCURITÉ DES RÉSEAUX ET DES SYSTÈMES D'INFORMATION DANS L'UNION

1. ETAT DU DROIT

1.1 Contexte d'adoption de la directive

Annoncée par la Commission européenne dès l'année 2010 avec la publication d'une Communication sur la stratégie numérique pour l'Europe[1], la directive concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et de l'information dans l'Union a été présentée par la Commission européenne (CE) début 2013[2].

Cette directive, première initiative de l'Union européenne (UE) visant à légiférer de façon globale dans le champ de la cyber-sécurité[3], s'inscrit dans une stratégie européenne qui a donné lieu à une publication concomitante de la Commission européenne et de la Haute représentante de l'Union européenne pour les affaires étrangères et la politique de sécurité[4].

La directive vise à répondre à l'un des objectifs de cette stratégie qui est le renforcement de la cyber-résilience des réseaux et des systèmes d'information des infrastructures critiques – définie comme la capacité de ces réseaux et systèmes de fonctionner à un niveau suffisant pour permettre d'assurer la continuité des services qui en dépendent en cas d'attaques ou d'incidents les affectant – au sein de l'Union européenne.

La directive est prise sur le fondement de l'article 114 du Traité sur le fonctionnement de l'Union Européenne[5] en raison du rôle primordial que joue la résilience des réseaux et systèmes informatiques dans le fonctionnement du marché intérieur.

Elle vise à augmenter les capacités des Etats membres en matière de cyber-sécurité et à accroître la coordination en cas d'incidents transnationaux, grâce à l'amélioration du niveau de préparation et de coopération des Etats-membres et l'adoption, par les opérateurs d'infrastructures critiques (telles que les réseaux d'énergie et de transports ou encore les principaux prestataires de services de la société de l'information) des mesures appropriées pour gérer les risques de sécurité et signaler les incidents graves aux autorités nationales compétentes.

---

[1] Document COM(2010) 245 final du 19.5.2010

[2] Document COM(2013) 48 final du 7.2.2013

[3] Définie par la directive comme la capacité des réseaux et des systèmes d'information de résister, à un niveau de confiance donné, à des actions qui compromettent la disponibilité, l'authenticité, l'intégrité ou la confidentialité de données stockées, transmises ou faisant l'objet d'un traitement, et des services connexes que ces réseaux et systèmes d'information offrent ou rendent accessibles.

[4] Document JOIN(2013) 1 final du 7.2.2013

[5] L'article 114 prévoit que l'Union européenne est habilitée à adopter des mesures destinées à établir ou assurer le fonctionnement du marché intérieur.

La Commission s'appuyait sur les constats suivants :

- la sécurité des réseaux et de l'information revêt une importance de plus en plus grande pour l'économie et la société. Elle est aussi une condition préalable importante à la création d'un environnement fiable pour le commerce international des services. Le manque de cyber-sécurité peut empêcher le fonctionnement des entreprises, entraîner des pertes financières considérables pour l'économie de l'Union Européenne et avoir une incidence négative sur le bien-être sociétal ;
- les systèmes d'information, et notamment l'internet, sont des instruments de communication sans frontière interconnectés entre les Etats membres et ils revêtent une importance essentielle pour la circulation transfrontière des biens, des services et des personnes. Toute perturbation importante de ces systèmes dans un Etat membre peut avoir une incidence sur d'autres Etats membres et sur l'UE dans son ensemble. La résilience et la stabilité des réseaux et systèmes informatiques sont donc essentielles pour l'achèvement du marché unique du numérique et le fonctionnement harmonieux du marché intérieur ;
- les moyens disponibles et les niveaux de préparation sont très différents selon les Etats membres, ce qui se traduit par une fragmentation des approches dans l'UE. Etant donné que les réseaux et systèmes informatiques sont interconnectés, c'est l'ensemble de la cyber-sécurité de l'UE qui peut être affaiblie par les Etats membres dont le niveau de protection est insuffisant ;
- il n'existe actuellement aucun véritable cadre au niveau de l'UE dans lequel pourraient s'inscrire la coopération et la collaboration ainsi que le partage d'informations de confiance sur les risques et incidents de cyber-sécurité entre les Etats membres ;
- les opérateurs qui gèrent des infrastructures critiques ou qui fournissent des services essentiels au fonctionnement de la société ne sont pas soumis à des obligations appropriées en ce qui concerne l'adoption de mesures de gestion des risques et l'échange d'informations avec les autorités compétentes ;
- une large proportion d'incidents n'est pas signalée aux autorités compétentes et passe inaperçue. Or, il est essentiel que les pouvoirs publics soient informés des incidents pour qu'ils puissent réagir, prendre les mesures d'atténuation nécessaires et fixer des priorités stratégiques adéquates en matière de cyber-sécurité.

Elle fixait à la directive pour principaux objectifs :

- d'instaurer des exigences minimales communes de cyber-sécurité au niveau national qui obligeraient les Etats membres à désigner des autorités nationales compétentes en la matière, à constituer une équipe d'intervention en cas d'urgence informatique (centre de réponse aux incidents de sécurité informatique) performante et à adopter une stratégie nationale et un plan national de coopération pour la cyber-sécurité ;
- d'instaurer des mécanismes de prévention, de détection, de remédiation et d'intervention permettant aux autorités nationales compétentes en matière de cyber-sécurité de partager des informations et de se porter mutuellement assistance. Il sera demandé à ces autorités

nationales compétentes d'assurer une coopération appropriée à l'échelle de l'UE, notamment à l'aide d'un plan de coopération de l'Union en la matière, permettant d'intervenir en cas de cyber-incident de dimension transnationale ;

– d'imposer aux opérateurs dans un certain nombre de secteurs importants pour le fonctionnement de l'économie et de la société d'évaluer les risques en termes de cyber-sécurité, d'assurer la fiabilité et la résilience des réseaux et systèmes informatiques par une gestion appropriée des risques et de signaler aux autorités nationales compétentes en matière de cyber-sécurité les incidents ayant un impact significatif sur la continuité des services essentiels et la fourniture des biens dépendant de réseaux et systèmes informatiques.

Compte tenu de la dimension transnationale des incidents et des risques de cyber-sécurité, la Commission estimait qu'il était approprié de développer une action au niveau de l'Union, dans le respect du principe de subsidiarité et que, conformément au principe de proportionnalité, la directive proposée n'excédait pas ce qui est nécessaire pour atteindre ces objectifs[6].

1.2 Etat des lieux

1.2.1 Au niveau européen

L'agence européenne pour la sécurité des réseaux (ENISA) a produit, en 2016, une analyse qui synthétise les résultats d'une vingtaine d'études sur les coûts économiques des cyber-incidents[7]. En dépit du constat de la difficulté d'interprétation et de comparaison des chiffres fournis par ces études, qui, compte tenu de l'absence de méthodologie commune, ne permettent pas d'évaluer de façon véritablement fiable l'impact économique de ces incidents et donc de prendre des mesures de sécurité appropriées, l'ENISA retenait les chiffres suivants :

- le coût global des incidents cybernétiques pourrait atteindre 1,6 % du PIB en Allemagne, ce chiffre ne serait que de 0,41 % au niveau de l'union européenne ;
- le coût sur les entreprises britanniques serait de 37 milliards d'euros par an. Des études indiquent que le coût annuel moyen pour une entreprise britannique, allemande ou française serait estimé dans une fourchette comprise entre quelques centaines de milliers d'euros et une vingtaine de millions d'euros. Une autre étude évalue le coût moyen annuel par entreprise sur un panel de 257 entreprises internationales de 0,5 million d'euros à 55 millions d'euros ;
- une étude chiffre le coût mondial dans une fourchette de 330 à 506 milliards d'euros.

Si ces chiffres doivent être considérés avec prudence, toutes les études convergeaient sur le fait que l'augmentation rapide des coûts induits par les cyber-incidents justifiait une action de l'Union européenne.

[6] La proposition de directive a été accompagnée d'une étude d'impact (document SWD (2013) 32 final du 7.2.2013.
[7] *The cost of incidents affecting CIIs* (disponible sur le site internet de l'ENISA).

La directive (UE) 2016/1148 du Parlement européen et du Conseil, du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union, communément appelée directive « NIS », a été adoptée après trois ans de négociation.

Sans en remettre en cause les objectifs principaux, les modifications apportées au texte initial visaient à atteindre l'équilibre entre l'instauration d'un cadre au niveau européen en matière de cyber-sécurité – ce, notamment, s'agissant de la coopération opérationnelle et politique entre les Etats membres – et la préservation de la souveraineté des Etats membres dans ce domaine. En outre, les dispositions concernant les fournisseurs de services numériques (places de marché en ligne, moteurs de recherche en ligne, service d'informatique en nuage) qui jouent un rôle majeur dans le fonctionnement de l'économie et de la société[8] sont allégées par rapport à celles applicables aux opérateurs de services essentiels. Enfin, les administrations publiques, qui figuraient dans le texte initial de la Commission, ont été exclues du champ d'application de la directive[9] exceptées lorsque celles-ci sont identifiées en tant qu'opérateurs de services essentiels.

Structurée autour de quatre axes, la directive prévoit :

– le renforcement des capacités des Etats membres en matière de cyber-sécurité (chapitre II). Les Etats membres devront notamment se doter d'autorités nationales compétentes en matière de cyber-sécurité, d'équipes nationales de réponse aux incidents informatiques (CSIRT) et de stratégies nationales de cyber-sécurité. L'annexe I de la directive précise les missions des CSIRT ;

– l'établissement d'un cadre de coopération volontaire entre les Etats membres (chapitre III). Cette coopération s'exercera à travers un « groupe de coopération » sur les aspects politiques de la cyber-sécurité et un « réseau européen des CSIRT » sur les aspects techniques et opérationnels ;

– l'instauration d'un cadre réglementaire destiné à renforcer la cyber-sécurité des opérateurs fournissant des services essentiels au fonctionnement de l'économie et de la société (chapitre IV). Ces opérateurs devront évaluer les risques et prendre des mesures de sécurité appropriées pour garantir la fourniture de leurs services. Ils notifieront les incidents de sécurité à l'autorité compétente et pourront être contrôlés. Les secteurs d'activités de ces opérateurs figurent à l'annexe II de la directive ;

– l'instauration d'un cadre réglementaire destiné à renforcer la cyber-sécurité des fournisseurs de services numériques (chapitre V). Ces fournisseurs seront tenus d'assurer la sécurité de leurs services, de notifier les incidents et pourront être contrôlés. L'annexe III de la directive précise les types de services numériques concernés.

La directive a été publiée au Journal officiel de l'UE le 19 juillet 2016 et est entrée en vigueur 20 jours après cette date. Elle devra être transposée d'ici au 9 mai 2018.

[8] Cf. services visés à l'annexe III de la directive et qui font l'objet de son chapitre V.

[9] Les administrations publiques étaient explicitement visées par le chapitre IV de la proposition initiale de directive de la Commission européenne.

La directive ainsi adoptée permet de concrétiser l'engagement fort de la France pendant toute la phase de négociation. La France a, en effet, été l'un des premiers pays européens à légiférer pour protéger les systèmes d'informations sensibles de ses opérateurs d'importance vitale[10]. Forte de son expérience quant à la cyber-sécurité des infrastructures critiques vitales pour la sécurité de la nation, elle a joué un rôle moteur dans la définition des orientations stratégiques de l'Union européenne en matière de cyber-sécurité et le dispositif français a d'ailleurs largement inspiré les principes de la présente directive.

1.2.2 Au niveau national

La France dispose déjà d'une autorité nationale compétente en matière de sécurité des réseaux et des systèmes d'information. En effet, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) créée par le décret n° 2009-834 du 7 juillet 2009 assure la fonction d'autorité de défense et de sécurité des systèmes d'information. A ce titre, elle a notamment pour mission :

- de proposer au Premier ministre les mesures destinées à répondre aux crises affectant ou menaçant la sécurité des systèmes d'information des autorités publiques et des opérateurs d'importance vitale ;
- de coordonner l'action gouvernementale dans le cadre des orientations fixées par le Premier ministre en matière de défense des systèmes d'information ;
- de proposer les mesures de protection des systèmes d'information ;
- de mener des inspections des systèmes des services de l'Etat et des opérateurs d'importance vitale ;
- de participer aux négociations internationales et d'assurer la liaison avec ses homologues étrangers.

L'Agence assure aussi une fonction de centre de réponse et de traitement des incidents de sécurité (CSIRT).

Compte tenu de son rôle central, l'ANSSI a donc naturellement vocation à être au cœur du dispositif de transposition.

Il existe en outre, dans le droit national, des dispositions destinées à renforcer la sécurité des systèmes d'information de certaines catégories d'opérateurs :

- pour les opérateurs de communications électroniques (articles L. 33-10, L. 33-1, et D. 98-5 du code des postes et des communications électroniques, qui transposent la directive 2002/21/CE relative à un cadre réglementaire commun pour les réseaux et services de communications électroniques) ;

[10] Articles L. 1332-6-1 et suivants du code de la défense issus de la loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale.

- pour les opérateurs d'importance vitale11 (articles L. 1332-6-1 et suivants du code de la défense, introduits par la loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019).

2. Objectifs poursuivis

L'objectif général de la directive est de garantir la continuité des activités économiques et sociétales critiques de la nation en cas de cyber-attaques qui, lorsqu'elles visent certaines entreprises stratégiques, notamment les opérateurs fournissant des services essentiels au maintien de l'activité économique et sociétale, constituent une menace pour la stabilité et la prospérité économique de l'Union. Il appartient donc à chaque Etat membre de renforcer le niveau de sécurité des réseaux et des systèmes d'information de ces opérateurs pour garantir la continuité des échanges au sein du marché intérieur et la compétitivité de l'Union dans le commerce international.

Les cyber-attaques visent aussi les fournisseurs de service numérique qui ont un rôle clé dans le fonctionnement quotidien de l'économie et de la société en raison de l'importance croissante du numérique. Ces services sont eux-mêmes souvent utilisés par les opérateurs de services essentiels.

L'objectif de la France est donc de renforcer la sécurité des systèmes d'informations de ces opérateurs et fournisseurs de service numérique, qui ne sont soumis actuellement à aucun dispositif réglementaire.

La France pourra, en outre, développer ses relations au niveau européen en participant activement au groupe de coopération prévu à l'article 11 de la directive et au réseau des CSIRT prévu à l'article 12. En termes d'organisation nationale, l'ANSSI jouera un rôle central.

Le tableau suivant synthétise les objectifs poursuivis par les différentes dispositions de la directive qui appellent à prendre des mesures législative ou réglementaire de transposition ou simplement des mesures d'application :

Chapitre I **Dispositions générales**	**Article 5 : Identification des opérateurs de services essentiels** Les Etats membres doivent identifier au plus tard le 9 novembre 2018 les opérateurs de services essentiels sur leur territoire. Chaque Etat membre doit désigner une autorité compétente nationale chargée d'identifier ces opérateurs sur la base des critères prévus à l'article 5.
Chapitre II **Cadres nationaux sur la sécurité des réseaux et des systèmes d'information**	**Article 7 : Stratégie nationale en matière de sécurité des réseaux et des systèmes d'information** Chaque Etat membre doit adopter une stratégie nationale qui définit les objectifs stratégiques et les mesures politiques et réglementaires appropriées en vue de parvenir à un niveau élevé de sécurité des réseaux et des systèmes d'information.

[11] Les opérateurs d'importance vitale sont définis aux articles L. 1332-1 et L. 1332-2 du code de la défense.

	Article 8 : Autorités nationales compétentes et point de contact unique Chaque Etat membre doit désigner une ou plusieurs autorités compétentes en matière de sécurité des réseaux et des systèmes d'information chargées de l'application de la directive au niveau national. Chaque Etat membre désigne aussi l'autorité qui le représentera dans le groupe de coopération prévu à l'article 11. Chaque Etat membre doit désigner un point de contact national unique chargé d'assurer la liaison avec les autorités des autres Etats membres.
	Article 9 : Centres de réponse aux incidents de sécurité informatique (CSIRT) Chaque Etat membre doit désigner un ou plusieurs CSIRT chargés de la gestion des incidents et des risques. Ces CSIRT coopèrent au sein du réseau européen des CSIRT prévu à l'article 12.
Chapitre III **Coopération**	Les Etats membres devront être représentés dans les deux instances de coopération prévues par ce chapitre : – **un groupe de coopération** (article 11) créé aux fins de soutenir et de faciliter la coopération stratégique et l'échange d'informations entre les autorités compétentes des Etats membres ; – **un réseau des CSIRT** (article 12) créé aux fins de promouvoir une coopération opérationnelle rapide et effective entre les CSIRT des Etats membres.
Chapitre IV **Sécurité des réseaux et des systèmes d'information des opérateurs de services essentiels**	**Article 14 : Exigences de sécurité et notification d'incidents** Les Etats membres doivent veiller à ce que les opérateurs de services essentiels prennent des mesures techniques et organisationnelles pour gérer les risques en matière de cyber-sécurité et pour prévenir les incidents de sécurité et notifient à l'autorité compétente les incidents de sécurité qui ont un impact significatif sur les services essentiels qu'ils fournissent.
	Article 15 : Mise en œuvre et exécution Les Etats membres doivent disposer des moyens pour contrôler le respect des exigences applicables aux opérateurs de services essentiels et pour contraindre ces opérateurs à respecter ces exigences.
Chapitre V **Sécurité des réseaux et des systèmes d'information des fournisseurs de service numérique**	**Article 16 : Exigences de sécurité et notification d'incidents** Les Etats membres doivent imposer aux fournisseurs de service numérique de prendre des mesures techniques et organisationnelles pour gérer les risques en matière de cyber-sécurité et pour prévenir les incidents de sécurité et de notifier à l'autorité compétente les incidents de sécurité qui ont un impact significatif sur les services numériques qu'ils fournissent.
	Article 17 : Mise en œuvre et exécution Les Etats membres doivent disposer des moyens pour contrôler le respect des exigences applicables aux fournisseurs de service numérique et pour contraindre ces fournisseurs à respecter ces exigences.

Chapitre VI Normalisation et notification volontaire	**Article 19 : Normalisation** Les Etats membres doivent encourager pour la mise en œuvre des mesures techniques et organisationnelles prévues aux articles 14 et 16 le recours à des normes européennes ou internationales en matière de cyber-sécurité.
	Article 20 : Notification volontaire Toute entité non identifiée comme opérateur de services essentiels ou fournisseur de service numérique pourra notifier à une autorité compétente, lorsqu'il est dans l'intérêt public de le faire, un incident ayant un impact significatif sur les services que cette entité fournit.
Chapitre VII Dispositions finales	**Article 21 : Sanctions** Des sanctions doivent être prévues en cas d'infractions aux obligations fixées par la directive.
	Article 25 : Transposition Les Etats membres doivent transposer au plus tard le 9 mai 2018 la présente directive et communiquer à la Commission européenne les textes de transposition.

3. Options possibles pour la transposition et nécessité de légiférer

Seules les dispositions relatives à la sécurité des réseaux et des systèmes d'information des opérateurs de services essentiels et des fournisseurs de service numérique sont de nature législative ou réglementaire et doivent être transposées dans le droit national.

Ces dispositions, qui figurent principalement aux chapitres IV et V de la directive prévoient, en effet, que les Etat membres imposent à ces deux catégories d'opérateurs des obligations :

- en matière de gestion des risques qui menacent la sécurité des réseaux et des systèmes d'information qu'ils utilisent dans le cadre de leurs activités ;
- en matière de prévention et de notification des incidents affectant ces réseaux et systèmes.

Pour garantir l'effectivité de ces mesures, la directive impose, en outre, aux Etats membres de veiller à ce que les autorités compétentes disposent des pouvoirs et des moyens nécessaires pour évaluer le respect, par les opérateurs de services essentiels et les fournisseurs de service numérique, des obligations qui leur incombent, ainsi que les effets de ce respect sur la sécurité des réseaux et des systèmes d'information.

Le tableau de transposition précise dans le détail les dispositions de la directive qui doivent faire l'objet d'une telle transposition.

Comme évoqué *supra* (voir 1.2.2), des dispositions relatives à la sécurité des systèmes d'information existent déjà dans le droit national pour les opérateurs de communications électroniques et pour les opérateurs d'importance vitale.

Ces dispositions ne permettent toutefois pas la transposition, dans le droit national, des dispositions applicables aux fournisseurs de services numériques et aux opérateurs de services essentiels.

En effet, la directive exclut, d'une part, de son champ d'application le secteur des communications électroniques (voir article 1er, al. 3) car il fait déjà l'objet d'une réglementation européenne équivalente dans ce domaine.

D'autre part, le dispositif applicable aux opérateurs d'importance vitale s'appuie sur des fondements juridiques et poursuit des finalités différentes de ceux de la directive dont le projet de loi poursuit la transposition.

Alors que la directive vise à assurer le fonctionnement des activités économiques et sociétales dans le cadre du marché intérieur, le dispositif applicable aux opérateurs d'importance vitale s'inscrit dans une stratégie de sécurité nationale de protection et de renforcement de la résilience de la Nation face aux risques majeurs. Les critères d'identification des opérateurs d'importance vitale définis aux articles L. 1332-1 et L. 1332-2 du code de la défense, sont, à cet égard, plus discriminants que ceux que donne la directive pour identifier un opérateur de service essentiel. Les premiers sont en effet définis, [à partir d'un critère physique] comme « des 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[12] » quand les seconds [identifiés à partir des services qu'ils fournissent et de la dépendance de ces services aux systèmes d'information] peuvent être désignés parmi des opérateurs économiques qui ne relèvent pas du domaine de la défense et de la sécurité nationale ou dont l'indisponibilité ne constituerait pas un « danger grave » pour la population[13].

Les obligations propres au dispositif existant dans le code de la défense seraient, en outre, inadaptées ou trop contraignantes pour ces opérateurs économiques. Dispositif global de protection face aux actes malveillants ou aux risques naturels, technologiques et sanitaires, il prévoit un ensemble d'obligations en matière de protection physique des installations sensibles (appelées « points d'importance vitale »), qui ne sont pas l'objet de la directive. Il impose de surcroît aux opérateurs concernés, pour des raisons de sécurité nationale, des obligations en matière d'habilitation au secret de la défense nationale ainsi que des mesures particulièrement exigeantes en matière de cyber-sécurité (telle que la mise en place d'un système de détection d'incidents prévue à l'article L. 1332-6-1 du code de la défense) qui seraient inadaptées pour des opérateurs qui ne seraient pas d'importance vitale pour la nation.

Enfin ce qui est vrai pour les opérateurs de service essentiel, l'est *a fortiori* pour les fournisseurs de service numérique, qui ne sont pas dans le champ du dispositif applicable aux opérateurs d'importance vitale tel qu'il est défini aux articles L. 1332-1 et suivants du code de la défense.

---

[12] Ou comme ceux exploitant des installations « dont la destruction ou l'avarie […] peut présenter un danger grave pour la population »

[13] Certains secteurs d'activités des opérateurs d'importance vitale et des opérateurs de services essentiels étant néanmoins communs, l'articulation entre ce dispositif et celui transposant la directive est analysée au point 4.2.

En conséquence, en l'absence de dispositions applicables dans le droit national, la transposition du chapitre V de la directive nécessite de prendre de nouvelles dispositions législatives qui s'articulent autour de deux volets, présentés ci-après (voir 4.2), l'un applicable aux opérateurs de service essentiel, l'autre applicable aux fournisseurs de service numérique.

4. Analyse des impacts des dispositions envisagées

4.1 Impact juridique

Le projet de loi crée de nouvelles dispositions qui ne seront pas codifiées. Ces dispositions, qui ne modifient aucune disposition existante, s'articulent de la manière suivante :

- des dispositions communes liminaires précisent les définitions de réseaux et systèmes d'information et de sécurité des réseaux et des systèmes d'information. Elles déterminent les règles applicables en matière de confidentialité et l'articulation des régimes nouvellement créés avec ceux que la directive exclut de son champ d'application.
- ces dispositions comportent, en deuxième lieu, des dispositions relatives à la sécurité des réseaux et systèmes d'information des opérateurs de service essentiel. Désignés individuellement par le Premier ministre à partir d'une liste de services essentiels fixée par décret, ces opérateurs seront tenus de respecter des règles de sécurité nécessaires à la protection de leurs réseaux systèmes d'information ;
- elles imposent, en troisième lieu, aux fournisseurs de service numérique opérant sur le territoire de l'Union européenne et ayant en France leur établissement principal ou leur représentant, d'identifier les risques qui menacent la sécurité de leurs réseaux systèmes d'information et de prendre les mesures techniques et organisationnelles nécessaires et proportionnées pour gérer ces risques, éviter la survenue d'incidents et en limiter les impacts.

Opérateurs de service essentiel et fournisseurs de service numérique devront déclarer les incidents affectant leurs réseaux et systèmes d'information et se soumettre, à la demande du Premier ministre, à des contrôles diligentés par l'ANSSI ou un prestataire de service habilité, destinés à vérifier le respect de leurs obligations en matière de sécurité des réseaux et systèmes d'information. Une mise en demeure de corriger les manquements constatés à l'issue de ce contrôle pourra être adressées aux fournisseurs et opérateurs.

Des sanctions pénales, enfin, pourront être appliquées en cas de manquement aux obligations fixées par la loi, ou d'obstacle aux contrôles effectués en application de celle-ci.

L'adoption de ces dispositions garantira la conformité de notre droit national au droit de l'Union européenne, sans créer, à l'égard des opérateurs auxquels elles s'appliqueront, d'obligations excédant ce qui est nécessaire à cette mise en conformité. Le dispositif de transposition proposé est néanmoins conçu (s'agissant en particulier des dispositions de la directive applicables aux opérateurs fournissant des services essentiels pour le fonctionnement

de l'économie et de la société) pour s'appliquer à un champ large d'opérateurs sans se restreindre *a priori* au champ minimal prévu par l'annexe II de la directive.

Cette approche est conforme à l'esprit de la directive qui définit un socle minimal commun de règles aux Etats membres sans interdire de prendre des dispositions complémentaires pour renforcer le niveau de sécurité (voir sur ce point le principe de l'harmonisation minimale prévu à l'article 3 de la directive).

Cela conduira à élargir progressivement, dans le respect des objectifs de la directive, la liste des secteurs et des services essentiels pour l'économie et la société au-delà des seuls secteurs fixés à l'annexe II de cette directive et ainsi à renforcer le niveau de cyber-sécurité de nouveaux opérateurs intervenant dans un champ économique et sociétal qui, bien qu'essentiels, échappent à ce jour, à toute réglementation en matière de cyber-sécurité.

En revanche, certains secteurs d'activités des opérateurs de services essentiels étant communs à ceux des opérateurs d'importance vitale, le projet de loi prévoit que ses dispositions ne sont pas applicables aux systèmes d'information déjà soumis aux règles fixées en application de l'article L. 1332-6-1 du code de la défense.

Les conditions d'application de ce dispositif seront fixées par décret (voir 6.1 Textes d'application). L'attribution de nouvelles missions à l'ANSSI pour la mise en œuvre du dispositif (voir 4.4 Impacts administratifs) impliquera, enfin, une modification du décret n° 2009-834 susmentionné [14] qui fixe les missions principales de l'ANSSI.

4.2 Impact économique

Le projet de loi impose de nouvelles obligations aux opérateurs de services essentiels et aux fournisseurs de service numérique.

Les coûts découleront pour l'essentiel des mesures de cyber-sécurité à mettre en place pour renforcer le niveau de sécurité et prévenir les incidents. Les mesures imposant de notifier des incidents de sécurité ou de se soumettre à des contrôles auront des coûts marginaux.

4.2.1 Coûts pour les opérateurs de services essentiels

Une fois la liste des services essentiels fixée par décret, les opérateurs seront désignés individuellement par le Premier ministre de façon progressive. La directive ne fixe pas de critères ou de seuils quantitatifs à prendre en compte pour identifier ces opérateurs. Les Etats membres restent libres d'apprécier le caractère « essentiel » des services fournis par les opérateurs et sont simplement tenus de désigner des opérateurs, *a minima* dans les secteurs mentionnés à l'annexe II de la directive. Sur la base d'un premier recensement, il est envisagé que le nombre d'opérateurs de services essentiels (incluant les opérateurs d'importance vitale) pourrait être de l'ordre de quelques centaines dans un premier temps. Les opérateurs du secteur privé se répartiront principalement entre des grandes entreprises et des entreprises de taille intermédiaire dans les secteurs de la santé, du transport, de l'industrie, de l'énergie, de l'alimentation, mais aussi de la logistique ou encore dans le secteur social. Les petites et

[14] Décret n° 2009-834 du 7 juillet 2009 portant création d'un service à compétence nationale dénommé « Agence nationale de la sécurité des systèmes d'information ».

moyennes entreprises seront très peu représentées. Dans le secteur public, les opérateurs seront essentiellement des établissements publics.

Le projet de loi prévoit d'imposer à ces opérateurs des règles de sécurité qui seront fixées au niveau réglementaire. Il s'agira d'un socle de règles de base (communément qualifiées de « règles d'hygiène ») permettant de mieux protéger les systèmes d'information contre la majorité des attaques observées actuellement. La mise en conformité avec ces règles sera fortement corrélée au niveau de maturité de chaque opérateur en matière de cyber-sécurité. Si l'opérateur a mis en œuvre une politique de sécurité adaptée, s'est doté d'équipements de sécurité et dispose de personnel formé, le coût sera sensiblement réduit voire marginal. Les coûts seront ainsi d'autant plus faibles que les opérateurs mettent déjà en œuvre les recommandations de sécurité de l'ANSSI.

Le coût de la mise en œuvre des règles sera précisé dans la fiche d'impact qui accompagnera le texte réglementaire fixant ces règles. Déjà évalué dans le cadre du dispositif applicable aux opérateurs d'importance vitale, ce coût s'échelonne de 1 à 2 millions d'euros par opérateur et par an, mais devrait être nettement plus faible s'agissant d'opérateurs de services essentiels, eu égard au caractère moins contraignant des règles qui leur seront appliquées.

4.2.2 Coûts pour les fournisseurs de service numérique

Les fournisseurs de service numérique ne seront pas désignés par l'autorité administrative. Ils s'identifieront eux-mêmes au regard de la définition de ces fournisseurs donnée par la directive et reprise à l'identique dans le projet de loi. La directive fixe les types de services numériques en annexe III mais sans préciser davantage de critères ou seuils quantitatifs. Il est simplement précisé que les microentreprises et petites entreprises sont exclues du champ. Par ailleurs, ces fournisseurs de service numérique étant pour la plupart établis à l'étranger[15],, l'article 18 de la directive prévoit un critère de compétence territoriale en fonction du lieu d'établissement du représentant de ces fournisseurs. L'application de la loi française aux fournisseurs de services numériques dépendant du choix autonome de ces entreprises quant à l'Etat dans lequel elles établiront leur représentant, l'estimation du nombre de fournisseurs concernés par la nouvelle réglementation française est malaisée. Il est vraisemblable, cependant, au vu du marché actuel que le projet de loi ne concernera au plus que quelques dizaines d'entreprises principalement d'origine étrangère.

Adoptant une approche moins prescriptive que celle proposée pour les opérateurs de services essentiels, conforme en cela à l'esprit de la directive qui se veut plus souple pour les fournisseurs de service numérique, le projet de loi ne fixe aux fournisseurs de service numérique qu'un objectif de résultat, les laissant libres de définir leurs propres mesures de sécurité. Le coût des mesures effectivement mises en place par ces fournisseurs ne pourra donc s'apprécier qu'à l'occasion des contrôles.

[15] Les principaux fournisseurs étrangers sont d'origine américaine (Google, Amazon, Microsoft,…).

4.2.3 Gains indirects

Si le projet de loi implique des coûts, le renforcement du niveau de sécurité doit permettre de bloquer les cyber-attaques ou d'en limiter les conséquences et ainsi de réduire les pertes financières qui résulteraient de cyber-attaques.

Aussi il convient de prendre en compte dans l'impact économique global du projet de loi les dommages financiers subis par les opérateurs en cas d'incidents informatiques d'origine malveillante ou non. Les coûts des dommages potentiels résultant d'un incident informatique correspondent aux coûts liés à l'indisponibilité et la reconstruction des systèmes d'information. Ils pourraient être bien supérieurs si d'autres types de dommages tels que l'atteinte à l'image, la perte de marchés ou encore le vol d'informations sensibles étaient également pris en considération.

Dans le cadre des interventions que l'ANSSI mène auprès de victimes de cyber-attaques, il est apparu que le coût des dommages directs (indisponibilité et reconstruction des systèmes) atteint couramment, en fonction de la taille de l'entreprise, un montant de quelques millions d'euros à quelques dizaines de millions d'euros pour une seule cyber-attaque réussie. De façon générale, les entreprises communiquent très peu sur les attaques et sur leur coût pour ne pas révéler leur vulnérabilité et pour protéger leur image. A titre d'exemple, toutefois, l'entreprise Saint-Gobain a évalué ses pertes financières à 250 millions d'euros sur les ventes de l'année 2017 en raison de la cyber-attaque NotPetya. L'entreprise TV5 a, quant à elle, évalué à 4,6 millions d'euros le coût de l'attaque qu'elle a subie en 2015.

Le coût des cyber-attaques est donc à mettre en regard du coût mentionné plus haut (moins de 1 à 2 millions d'euros annuels) pour mettre en œuvre les règles de sécurité.

4.3 Impact social

L'actualité récente a montré que tous les secteurs d'activité pouvaient être victimes d'attaques informatiques d'envergure, susceptibles de ralentir ou paralyser l'activité de pans entiers de l'économie au-delà des frontières d'un Etat.

L'entreprise américaine *YAHOO!* a annoncé aux mois de septembre et décembre 2016 avoir été victime de plusieurs compromissions de son système d'information. Deux compromissions majeures datant d'août 2013 et de 2014 ont abouti à l'exfiltration massive de données personnelles liées à près d'un milliard de comptes d'utilisateurs du service de messagerie. En août 2016, près d'un milliard d'adresses liées à des comptes de messagerie *YAHOO!*, potentiellement issues de l'exploitation de ces deux compromissions, ont été mises en vente sur le marché noir.

Le 6 décembre 2016, la bourse, le fonds de pension national, l'autorité maritime et l'autorité des chemins de fer ukrainiens ont été les victimes d'un sabotage informatique. Ces opérations de sabotage informatique ont été réalisées suivant un mode opératoire déjà observé en décembre 2015 lors des attaques par sabotage à l'encontre du réseau de distribution d'électricité en Ukraine.

Début 2016, une campagne d'attaques informatiques sophistiquées et planifiées a ciblé des entités bancaires clientes de la plateforme de messagerie interbancaire SWIFT et principalement situées en Asie du Sud-Est. Une trentaine d'ordres de paiement frauduleux auraient ainsi été émis par les attaquants pour un montant total avoisinant un milliard de dollars. Bien que la plupart des virements frauduleux aient pu être annulés, les pertes totales dues à ces attaques s'élèvent à quatre-vingt-un millions de dollars.

Une augmentation importante du volume des attaques en déni de service distribué[16] (DDoS) a été observée en 2016. Ces attaques d'ampleur inédite ont pu être réalisées grâce à des *botnets* constitués de dizaines, voire de centaines, de milliers d'objets connectés compromis au moyen du code malveillant *MIRAI*. Les attaques du 21 octobre 2016 contre l'un des principaux services d'hébergement américains de sites Internet, *DYN*, ont provoqué l'inaccessibilité de plusieurs services Internet majeurs comme *TWITTER*, *NETFLIX* et *AMAZON*. L'hébergeur français *OVH* a également été victime de ce type d'attaques en septembre 2016.

Au-delà de l'impact direct sur le fonctionnement de l'économie et la société, le projet de loi favorisera le développement de l'industrie de la cyber-sécurité et augmentera les besoins en main-d'œuvre qualifiée dans ce secteur. Il donnera ainsi un élan au développement des services en matière de conseil, d'audit, de détection et de traitement d'incidents de cyber-sécurité et des produits de sécurisation des réseaux et des systèmes d'information, profitable à l'ensemble des entreprises de produits et de services de sécurité numérique dans l'ensemble du marché intérieur européen. L'ensemble de la filière cyber-sécurité bénéficiera donc de la mise en œuvre de ce projet de loi.

4.4 Impact administratif

L'ANSSI sera chargée de la mise en œuvre globale du dispositif. Elle recevra et traitera les incidents de sécurité qui lui seront déclarés, contrôlera les opérateurs et les fournisseurs de service numérique et de façon générale leur apportera un soutien pour mettre en œuvre les règles et mesures de sécurité. En outre, elle devra :

- élaborer la stratégie nationale prévue à l'article 7 de la directive en matière de sécurité des réseaux et des systèmes d'information, en cohérence avec la stratégie nationale pour la sécurité du numérique qui a été adoptée en 2015 ;
- assurer les fonctions d'autorité nationale compétente et de point de contact unique prévues à l'article 8 de la directive ;
- représenter la France dans le groupe de coopération prévu à l'article 11 et dans le réseau des CSIRT prévu à l'article 12.

[16] Une attaque de type DDOS est une attaque informatique ayant pour but de rendre indisponible un service ou un serveur (serveur de fichiers, serveur web, serveur de courriers, etc.) et d'empêcher ainsi les utilisateurs légitimes d'y accéder. Le type d'attaque DDOS le plus fréquent consiste pour l'attaquant à envoyer vers la cible un trafic très volumineux pour submerger la bande passante du serveur et ainsi rendre indisponible l'accès normal. En général, l'attaquant utilise pour cela un ensemble de machines (appelées « *botnet* ») dont il a pris le contrôle, souvent à l'insu de leurs utilisateurs, qui vont envoyer du trafic vers la cible.

Pour la mise en œuvre du dispositif, l'ANSSI pourra s'appuyer sur les moyens déjà mis en place pour le dispositif relatif aux opérateurs d'importance vitale. Toutefois, en fonction du nombre d'opérateurs de services essentiels potentiellement concernés par le nouveau dispositif, des ressources humaines supplémentaires pourraient être nécessaires. Dans une première étape ciblant quelques centaines d'opérateurs, cette charge devrait être absorbée par l'ANSSI grâce à la croissance des moyens de l'agence. Si le dispositif devait s'étendre largement au-delà de ce périmètre, des moyens supplémentaires devraient probablement être envisagés.

Les ministères qui assurent la tutelle des secteurs d'activités concernés, dont le rôle sera précisé par le décret d'application, seront naturellement impliqués, en relation avec l'ANSSI, dans la mise en œuvre de ce nouveau dispositif. Celui-ci n'engendrera néanmoins pour les ministères concernés, qu'une charge de travail marginale.

4.5 Impact environnemental

Le projet de loi n'a aucun impact environnemental direct. Toutefois, en améliorant le niveau de sécurité de certains opérateurs intervenant dans des domaines liés à l'environnement tels que l'énergie et le transport, le projet de loi contribuera à limiter les risques environnementaux en cas d'incidents d'origine informatique affectant les systèmes de ces opérateurs. En effet, à titre d'exemple, les systèmes d'information permettant de piloter des installations de production, de raffinage, de transport de pétrole ou de gaz, ou ceux mis en œuvre pour gérer le transport de marchandises et matières dangereuses par voie maritime ou terrestre sont susceptibles d'être attaqués aux fins de créer des dommages environnementaux majeurs, que le renforcement de la sécurité de ces systèmes permettra de limiter.

5. Consultations menées

Aucune consultation obligatoire n'était nécessaire dans le cadre de la mise en œuvre du dispositif retenue.

En revanche, les textes d'application comporteront des mesures sectorielles à caractère technique, qui devront être soumis à certaines consultations obligatoires, notamment s'agissant des règles de sécurité applicables aux opérateurs de services essentiels.

Des consultations informelles avec des opérateurs de services essentiels susceptibles d'être désignés et des fournisseurs de service numérique pourront aussi être menées. Enfin, des échanges sont en cours avec les autres Etats membres afin de comparer les différentes approches envisagées pour la transposition de la directive par ces Etats. Ces échanges ont lieu dans le cadre du groupe de coopération instauré par la directive, qui permet notamment aux Etats membres de partager des informations sur la transposition de la directive.

6. Modalités de mise en œuvre

6.1 Textes d'application

Le projet de loi renvoie à un décret en Conseil d'Etat l'ensemble des conditions d'application. Le décret fixera notamment la liste des services essentiels pour chaque secteur d'activités des opérateurs de services essentiels. Ce décret renverra lui-même vers deux arrêtés pour fixer :

- la liste des règles de sécurité nécessaires à la protection des réseaux et systèmes d'information ;
- les coûts des contrôles destinés à vérifier le respect des obligations relatives à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels et des fournisseurs de service numérique.

Les opérateurs de service essentiel seront individuellement désignés par le Premier ministre. La liste de ces opérateurs sera actualisée au moins tous les deux ans. Enfin le décret n° 2009-834 du 7 juillet 2009 portant création d'un service à compétence nationale dénommé « Agence nationale de la sécurité des systèmes d'information » sera modifié en conséquence des nouvelles missions attribuées à l'ANSSI.

6.2 Application dans le temps

Conformément à ce que prévoit la directive, les dispositions de la loi entreront en vigueur au plus tard le 9 mai 2018, à l'exception de celles relative aux opérateurs de services essentiels, qui n'entreront en vigueur qu'à compter de la désignation de ces opérateurs, soit au plus tard le 9 novembre 2018.

6.3 Application dans l'espace

La loi s'appliquera sur l'ensemble du territoire de la République.

TITRE II - TRANSPOSITION DE LA DIRECTIVE (UE) 2017/853 DU PARLEMENT EUROPÉEN ET DU CONSEIL DU 17 MAI 2017 MODIFIANT LA DIRECTIVE 91/477/CEE DU CONSEIL RELATIVE AU CONTRÔLE DE L'ACQUISITION ET DE LA DÉTENTION D'ARMES

La directive 91/477/CEE du Conseil du 18 juin 1991 relative au contrôle de l'acquisition et de la détention d'armes avait pour objectif de faciliter le fonctionnement du marché intérieur des armes à feu sur le territoire de l'Union, tout en garantissant un niveau élevé de sécurité pour les citoyens européens.

À cet effet, la directive établit les exigences minimales que devraient imposer les États membres en ce qui concerne l'acquisition et la détention d'armes à feu de chaque catégorie et fixe les conditions applicables aux transferts d'armes à feu entre États membres, tout en prévoyant des règles plus souples pour la chasse et le tir sportif[17].

La modification résultant de la directive 2008/51/CE du 21 mai 2008[18], a eu pour objet de renforcer les aspects liés à la sécurité et d'aligner la directive sur le protocole contre la fabrication et le trafic illicites d'armes à feu, de leurs pièces, éléments et munitions, additionnel à la Convention des Nations unies contre la criminalité transnationale organisée[19].

La directive (UE) 2017/853 du Parlement européen et du Conseil du 17 mai 2017 modifiant la directive 91/477/CEE du conseil relative au contrôle de l'acquisition et de la détention d'armes, publiée au Journal officiel de l'Union européenne le 24 mai 2017, s'inscrit, dans le prolongement de la directive de 2008, dans une logique de renforcement des mesures de sécurité. Au lendemain des attentats terroristes perpétrés à Paris en janvier 2015, a été adoptée la « Déclaration de Paris », dans laquelle les ministres de l'intérieur ou de la justice de l'Union européenne ont affirmé leur détermination à lutter contre la circulation illégale d'armes à feu sur l'ensemble du territoire européen et, dans cette optique, à renforcer leur coopération au sein de la plateforme pluridisciplinaire européenne contre les menaces

[17] Les États membres ont bien sûr le droit, en principe, de prendre des mesures plus strictes que celles prévues par la directive.

[18] Deux facteurs sont intervenus dans la décision de modifier la directive, à savoir :

a) la signature, par la Commission européenne au nom de la Communauté européenne, le 16 janvier 2002, du protocole des Nations unies contre la fabrication et le trafic illicites d'armes à feu, de leurs pièces, éléments et munitions, additionnel à la convention des Nations unies contre la criminalité transnationale organisée ;

b) les résultats et propositions d'amélioration (armes neutralisées, licences d'importation et d'exportation, tenue de registres, marquage, etc.) présentés par la Commission dans son rapport de décembre 2000 sur la mise en œuvre de la directive 91/477/CEE, faisant suite à la t transposition en droit national de celle-ci par tous les États membres – COM(2000) 837, rapport au Parlement européen et au Conseil, « Mise en œuvre de la directive 91/477/CEE du Conseil du 18 juin 1991 relative au contrôle de l'acquisition et de la détention d'armes », 15 décembre 2000.

[19] Protocole contre la fabrication et le trafic illicites d'armes à feu, de leurs pièces, éléments et munitions, additionnel à la Convention des Nations Unies contre la criminalité transnationale organisé, adopté par la résolution 55/255 de l'Assemblée générale des Nations Unies le 31 mai 2001 et entré en vigueur le 3 juillet 2005

criminelles (EMPACT), à améliorer le partage du renseignement et à utiliser pleinement les ressources d'Europol, d'Eurojust et d'Interpol[20].

Lors de la réunion informelle du Conseil européen du 12 février 2015, les chefs d'État ou de gouvernement ont demandé à toutes les autorités compétentes de renforcer leur coopération dans la lutte contre le trafic illicite d'armes à feu, notamment en révisant rapidement la législation applicable, et de relancer le dialogue sur les questions de sécurité avec les pays tiers, notamment ceux du Moyen-Orient et de l'Afrique du Nord, mais aussi des Balkans occidentaux[21].

À l'issue de la réunion du Conseil « Justice et affaires intérieures » des 12 et 13 mars 2015, les ministres ont invité la Commission à proposer de nouveaux moyens pour lutter contre le trafic illicite d'armes à feu et à intensifier, en collaboration avec Europol, l'échange d'informations et la coopération opérationnelle[22].

C'est pourquoi, la Commission a adopté le programme européen en matière de sécurité, destiné à permettre une réponse efficace et coordonnée à l'échelon européen face à l'apparition de menaces de plus en plus complexes pour la sécurité.

Parmi les actions prioritaires décrites dans ce programme, il est notamment recommandé de réexaminer la législation sur les armes à feu sur la base de propositions à formuler en 2016[23]. Le programme préconise en outre de prendre d'urgence les mesures qui s'imposent pour empêcher que des armes à feu neutralisées puissent être réactivées et utilisées par des criminels.

Dans leur déclaration du 29 août 2015, les ministres de l'intérieur européens ont une nouvelle fois plaidé en faveur de la révision de la directive sur les armes à feu et de l'élaboration de normes communes sur la neutralisation des armes à feu.

Enfin, le 8 octobre 2015, le Conseil a adopté ses conclusions sur l'application renforcée des moyens mis en œuvre pour lutter contre le trafic d'armes à feu, dans lesquelles il invite les États membres, la Commission européenne, Europol et Interpol à engager certaines actions, parmi lesquelles réviser la législation en vigueur et surveiller les menaces que représentent les armes à feu au moyen d'enquêtes et d'opérations transfrontières coordonnées. Cet appel à l'action concerne également les trafics d'armes à feu réalisés au moyen de l'internet.

Le Parlement européen a lui aussi examiné à de multiples reprises la question du trafic d'armes à feu. Le 11 février 2015, il a adopté une résolution sur les mesures de lutte contre le terrorisme, dans laquelle il demande à la Commission « *d'évaluer d'urgence les règles de l'Union en vigueur sur la circulation des armes à feu illicites, les explosifs et le trafic d'armes liés à la criminalité organisée* ».

L'essentiel de la transposition de la directive du 17 mai 2017, entrée en vigueur le 13 juin 2017, relève du domaine réglementaire.

[20] 5322/15, « Déclaration de Paris » du 11 janvier 2015.
[21] 6112/15, projet de déclaration des membres du Conseil européen.
[22] 7178/15, communiqué de presse du Conseil «Justice et affaires intérieures».
[23] COM(2015) 185 final du 28.4.2015.

La directive du 17 mai 2017 comporte néanmoins 6 six mesures nécessitant une transposition par voie législative.

- La disparition de la catégorie D des armes à feu (articles 4, 4 bis, 8, 12 et annexe I de la directive).
- Le nouveau régime des reproductions d'armes historiques ((b) du III de l'annexe I de la directive). La directive inclut désormais dans son champ d'application, les reproductions d'armes historiques, contrairement à ce que prévoyait la directive antérieure.
- L'instauration d'un contrôle administratif pour les courtiers d'armes de catégorie C (point 3 de l'article 4 et considérants 4 et 5 de la directive) : la directive soumet à réglementation toutes les activités d'armuriers et de courtiers.
- Les dérogations à l'interdiction d'acquisition et de détention d'armes de catégorie A (article 6 et annexe I de la directive). La directive (annexe I) surclasse des armes qui étaient jusqu'alors en catégorie B, soumises à autorisation, pour les passer en catégorie A, prohibées (sauf pour les forces de sécurité publique), mais elle ouvre aux États membres la possibilité de déroger pour certaines catégories de détenteurs à la prohibition d'acquisition et de détention de certaines de ces armes surclassées.
- L'interdiction de la livraison au domicile de l'acquéreur d'armes achetées par correspondance (article 5 ter de la directive). La directive n'a ni pour objet ni pour effet d'interdire les ventes d'armes au moyen de contrats à distance (internet, ventes par correspondance), mais elle fixe pour objectif que, dans ce cas, la livraison de l'arme fasse l'objet d'une vérification de l'identité de l'acheteur et, le cas échéant, de son autorisation d'acquisition et de détention, avant la livraison ou au plus tard, concomitamment à la livraison, soit auprès d'un armurier, soit auprès d'une autorité publique.
- Les transactions suspectes (article 10 de la directive). La directive prévoit une possibilité, pour les armuriers, de refuser légalement des transactions portant sur des munitions et composants de munitions qui apparaîtraient comme suspectes en raison de leur nature ou de leur échelle. Elle prévoit aussi un régime de signalement de ces tentatives de transaction. Pour des raisons de cohérence, il est proposé, sur ce point, d'aller au-delà des exigences strictes de la directive en étendant aux armes et éléments d'armes ce nouveau dispositif de transaction suspecte, qui n'existe pas, pour ces matériels, dans notre droit interne.

LA DISPARITION DE LA CATÉGORIE D DES ARMES À FEU DE LA DIRECTIVE

1. ETAT DES LIEUX ET DIAGNOSTIC DROIT

En France, les armes de chasse relèvent de deux catégories juridiques distinctes : la catégorie C soumise à déclaration ou la catégorie D 1° soumise à enregistrement. D'autres armes libres d'acquisition et de détention relèvent de la catégorie D 2°.

La procédure d'enregistrement a été créée par le décret n° 2011-1253 du 7 octobre 2011 modifiant le régime des matériels de guerre, armes et munitions. Ce texte avait pour objet de prévoir une procédure d'enregistrement de certaines armes de chasse pour en assurer la traçabilité et assurer ainsi la complète transposition de la directive 2008/51/CE du 21 mai 2008 du Parlement européen et du Conseil européen. Conformément à son article 18, cette procédure d'enregistrement s'applique uniquement aux armes « de chasse » reçues ou acquises à compter de l'entrée en vigueur du présent décret, ce qui signifie que le stock de ces armes n'est donc pas concerné par cette nouvelle formalité administrative.

La catégorie D des armes à feu est pour sa part mentionnée dans la partie II de l'annexe I de la directive du 18 juin 1991 modifiée. Cette catégorie comprend, selon l'annexe utile de la directive, « les armes à feu longues à un coup par canon lisse ». Il s'agit dans les faits d'une partie très importante des armes de chasse classiques, qui étaient donc soumises, en droit interne, au contrôle administratif « minimal » : le régime de l'enregistrement. A ce jour, environ 250 000 armes relevant de la catégorie D (1°) sont enregistrées dans l'application de gestion du répertoire informatisé des propriétaires et possesseurs d'armes (AGRIPPA)[24].

Jusqu'à la loi n°2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale, le régime d'enregistrement se distinguait de celui de la déclaration par le contrôle de l'honorabilité du demandeur : ce contrôle n'existait pas dans la procédure d'enregistrement, mais uniquement dans la procédure de déclaration. La loi du 3 juin 2016 a étendu le contrôle d'honorabilité à la procédure d'enregistrement, qui ne se distingue donc plus de celle de déclaration.

La directive du 17 mai 2017 susmentionnée marque une rupture. Elle supprime l'une des deux catégories (la catégorie D) pour n'en laisser qu'une seule (la catégorie C) soumise à un régime de déclaration. Si la catégorie D 1° va donc disparaître du fait de la directive, la catégorie D 2° a vocation à demeurer dans la partie réglementaire du code de la sécurité intérieure (R. 311-2 du CSI), et la référence à la catégorie D est maintenue dans la partie législative du code (L.311-2 du CSI), lorsque son champ couvre les armes de détention et d'acquisition libres.

[24] Arrêté du 15 novembre 2007 portant création de l'application de gestion du répertoire informatisé des propriétaires et possesseurs d'armes.

Classement des armes de chasse avant la directive du 17 mai 2017 :

Type d'armes / Classement	Armes à feu d'épaule à un coup par canon dont l'un au moins n'est pas lisse[25]	Armes d'épaule à canon lisse tirant un coup par canon
Classement par l'annexe à la directive du 18 juin 1991 modifiée par la directive 2008/51/CE du 21 mai 2008	Catégorie C : soumise à déclaration	Catégorie D : autres armes à feu
Classement par les articles L. 311-2 et R. 311-2 du code de la sécurité intérieure	Catégorie C : soumise à déclaration	Catégorie D (1°) : soumise à enregistrement

Classement des armes de chasse après la directive du 17 mai 2017 :

Type d'armes / Classement	Armes à feu d'épaule à un coup par canon dont l'un au moins n'est pas lisse	Armes d'épaule à canon lisse tirant un coup par canon
Classement par l'annexe à la directive du 18 juin 1991 modifiée par la directive (UE) 2017/853 du 17 mai 2017	Catégorie C : soumise à déclaration	Catégorie C : soumise à déclaration
Classement par les futurs articles du code de la sécurité intérieure	Catégorie C : soumise à déclaration	Catégorie C : soumise à déclaration

2. OBJECTIFS POURSUIVIS

La directive du 17 mai 2017 supprime la catégorie D ("Autres armes à feu") de la partie II de son annexe I. Les armes à feu qui y figuraient sont intégrées dans la catégorie C (armes soumises à déclaration). Cette catégorie comprenait les armes à feu longues à un coup par

[25] Cette formulation est utilisée car il existe en pratique des fusils de chasse appelés mixtes qui possèdent un canon lisse et un canon rayé (juxtaposés ou superposés). La directive du 18 juin 1991 modifiée utilise quant à elle l'expression suivante : « les armes à feu longues à un coup par canon rayé ».

canon lisse. Par conséquent, il n'existe plus que trois catégories d'armes à feu (A, B et C). L'esprit de la directive est de supprimer la formalité d'enregistrement des armes de catégorie D 1° pour la remplacer par la procédure de déclaration, ce qui contribue au renforcement de la sécurité publique.

L'objectif du projet de loi, sur ce point, est donc d'aligner les catégories d'armes nationales sur les catégories d'armes à feu prévues par la partie II de l'annexe I de la directive du 17 mai 2017. En outre, cet alignement a pour conséquence positive de supprimer la distinction de deux procédures administratives (celle de l'enregistrement et celle de la déclaration) qui étaient, de fait, devenues semblables après les modifications introduites par la loi n°2016-731 du 3 juin 2016[26].

3. NECESSITE DE LEGIFERER ET OPTION RETENUES

Les différentes catégories d'armes à feu sont énumérées par l'article L. 311-2 du code de la sécurité intérieure et par l'article L. 2331-1 du code de la défense. Le classement des armes au sein de ces catégories relève quant à lui du pouvoir réglementaire.

La suppression par la directive des armes de catégorie D nécessite donc des dispositions législatives sachant qu'aucune option n'est permise pour les États membres quant à la disparition de cette catégorie, puisque ceux-ci ne peuvent adopter que des mesures plus restrictives que celles fixées par la directive.

Les dispositions envisagées tirent les conséquences de la suppression de la catégorie D dans la partie législative du code de la sécurité intérieure et, par coordination, du code de la défense.

4. ANALYSE DES IMPACTS DES DISPOSITIONS ENVISAGEES

4.1 Impact juridique

Le classement actuellement en vigueur fait que les fusils à un coup par canon lisse sont soumis à enregistrement en préfecture conformément au 4° de l'article L. 311-2, au a) du 1° de l'article R. 311-2 du code de la sécurité intérieure et au 4° de l'article L. 2331-1 du code de la défense.

Les armes à feu qui sont actuellement soumises à enregistrement vont, par l'effet des modifications de la partie II de l'annexe I de la directive du 17 mai 2017, être intégrées dans la catégorie C, de ce fait soumises à déclaration. Il s'agit donc moins de la suppression d'une catégorie d'armes à feu que d'un surclassement de ces armes à feu.

26 Loi n° 2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale, relatives au renforcement du dispositif en matière de lutte contre le trafic d'armes.

Toutefois, les effets juridiques de ce surclassement par la directive sont à relativiser :

Comme cela a été précisé ci-dessus, il n'existe plus aujourd'hui, en effet, de différence entre le régime de déclaration (catégorie C) et le régime d'enregistrement (catégorie D 1°).

De ce point de vue, le passage de l'enregistrement (D) à la déclaration (C) ne change donc rien à la situation de fait des détenteurs de ces armes.

Il y a même une certaine cohérence à uniformiser les régimes de l'enregistrement et de la déclaration, qui avaient perdu en lisibilité depuis l'harmonisation des contrôles résultant de la loi du 3 juin 2016 précitée. Ce n'est bien sûr pas l'objet de la directive, mais c'est l'un de ses effets sur notre droit national.

La portée du surclassement de ces armes de chasse est par ailleurs précisément encadrée par la directive en révision :

- le changement n'aura aucun effet sur les détenteurs d'armes acquises avant le 1er décembre 2011[27] (date à compter de laquelle ces armes ont été soumises à enregistrement en France). Ces détenteurs n'auront aucune démarche à faire, et l'administration n'aura aucune action à entreprendre. La très grande majorité des détenteurs de ces armes de chasse est dans cette situation (on peut estimer qu'entre 1 et 3 millions d'armes sont dans ce cas). Ces détenteurs bénéficient en effet, au terme de la directive, d'une clause d'antériorité ;
- le changement concernera immédiatement, en revanche, les armes de ce type mises sur le marché après la transposition par la France de la directive révisée, dans le délai fixé par cette directive. La directive raisonne en effet, pour ces armes, en flux et non en stock.

Le flux peut être estimé à environ 40 000/an, si l'on se réfère aux enregistrements annuels de ces armes, constatés en préfecture depuis 2012.

Les chasseurs devront donc, pour les mises sur le marché postérieures à la transposition, déclarer leur arme (désormais en catégorie C), au lieu de la faire enregistrer (conformément à la catégorie D).

Or, comme il a été indiqué, ces procédures sont devenues strictement équivalentes depuis la loi du 3 juin 2016. Le changement sera donc administrativement neutre, plus formel que réel en quelque sorte, et pour les détenteurs et pour les préfectures, puisque le flux annuel restera probablement constant.

Enfin, les chasseurs qui auraient acquis une arme de ce type après le 13 juin 2017 (date d'entrée en vigueur de la directive du 17 mai 2017), sous un régime d'enregistrement, mais avant la date butoir de la transposition (14 septembre 2018) pourront, le cas échéant, bénéficier d'un délai allongé pour basculer sous un régime de déclaration : la directive autorise en effet, dans ce cas, un délai de mise en conformité jusqu'au 14 mars 2021.

[27] Décret n° 2011-1253 du 7 octobre 2011 modifiant le régime des matériels de guerre, armes et munitions.

Il reste que les détenteurs titulaires d'un récépissé d'enregistrement (environ 250.000 aujourd'hui) pourraient souhaiter une « sécurisation » de leur détention (par exemple, pour faire des déplacements au sein de l'Union pour la pratique de la chasse), en demandant un titre de détention faisant référence à la catégorie C et non plus à la catégorie D.

Des mesures réglementaires d'accompagnement pourraient être envisagées, comme l'assimilation du récépissé d'enregistrement au récépissé de déclaration.

Cette assimilation devrait satisfaire les représentants des détenteurs d'armes, consultés sur ce point.

4.2 Impact économique

On peut estimer que, compte tenu de l'absence d'effet juridique sensible du changement de régime et de la suppression de la catégorie D, il n'y aura pas d'impact économique pour les détenteurs de ces armes et pour les professionnels de ce secteur d'activité, ce type d'arme restant en tout état de cause l'archétype de l'arme de chasse.

4.3 Impact administratif

Les procédures d'enregistrement et de déclaration étant devenues strictement équivalentes depuis la loi du 3 juin 2016, le remplacement de la première procédure par la seconde sera neutre pour les services des préfectures[28], en charge de l'application de la réglementation relative aux armes et munitions, comme elles l'étaient auparavant pour le traitement des enregistrements. Le passage de la procédure d'enregistrement à la procédure de déclaration ne devrait pas en principe susciter de besoins en formation puisque la procédure de déclaration est déjà gérée par les préfectures.

S'agissant des détenteurs d'armes, les personnes qui, à la date d'entrée en vigueur de la présente loi, détiennent des armes acquises depuis le 13 juin 2017, date d'entrée en vigueur de la directive, qui étaient soumises à enregistrement au titre du 1° de la catégorie D et qui sont désormais classées dans la catégorie C soumise à déclaration, devront procéder à la déclaration de ces armes auprès du représentant de l'État dans le département.

5. MODALITÉS DE MISE EN ŒUVRE

5.1 Textes d'application

Le classement des armes au sein des différentes catégories définies par la loi relève du pouvoir réglementaire. Un décret en Conseil d'État sera notamment nécessaire pour :

- tirer les conséquences de la suppression de la catégorie D des armes à feu ;

- prévoir les dispositions transitoires nécessaires.

[28] Ces services sont divers : il peut s'agir de bureau des armes au sein du service du cabinet du préfet, de service des armes en sous-préfectures, de bureau de la réglementation au sein des directions de la réglementation et des libertés publiques, de directions des sécurités au sein des cabinets des préfectures.

5.2 Application dans le temps

Le projet de loi portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité introduit des dispositions relatives à l'entrée en vigueur des différents articles du titre II, consacré à la transposition de la directive (UE) 2017/853 du Parlement européen et du Conseil du 17 mai 2017.

Les dispositions envisagées entreraient en vigueur à compter d'une date définie par décret en Conseil d'État et au plus tard le 14 septembre 2018. Le décret définira les modalités d'application de ces dispositions, ainsi que les modalités permettant aux détenteurs de ces armes de régulariser, le cas échéant, leurs situations au regard des nouveaux classements.

Les personnes qui, à la date d'entrée en vigueur de la présente loi, détiennent des armes acquises depuis le 13 juin 2017, date d'entrée en vigueur de la directive, qui étaient soumises à enregistrement au titre du 1° de la catégorie D et qui sont désormais classées dans la catégorie C soumise à déclaration, devront procéder à la déclaration de ces armes auprès du représentant de l'État dans le département du lieu de leur domicile dans les conditions fixées par décret en Conseil d'État, et au plus tard le 14 décembre 2019. Le choix a été fait de ne pas attendre la date ultime, fixée par le 4 de l'article 2 de la directive au 21 mars 2021, pour organiser cette régularisation. Les considérations de sécurité publique conduisent à ne pas attendre une date aussi lointaine, et les considérations de gestion administrative, à ne pas imposer cette régularisation dès la transposition « de droit commun », c'est-à-dire le 14 septembre 2018.

5.3 Application dans l'espace

Les dispositions de la présente loi s'appliquent sur l'ensemble du territoire de la République et notamment en Nouvelle-Calédonie, en Polynésie française, dans les îles Wallis-et-Futuna et dans les Terres australes et antarctiques françaises.

Conformément au principe de spécialité législative, les modifications des dispositions du livre III du code de la sécurité intérieure et du livre III de la 2ème partie du code de la défense, faites par le titre II de la présente loi, doivent être rendues expressément applicables aux collectivités susmentionnées. Tel est l'objet des modifications prévues par les articles L. 344-1, L. 345-1, L. 346-1 et L. 347-1 du code de la sécurité intérieure et par les articles L. 2441-1, L. 2451-1, L. 2461-1 et L. 2471-1 du code de la défense.

LE NOUVEAU RÉGIME DES REPRODUCTIONS D'ARMES HISTORIQUES

1. ETAT DES LIEUX ET DIAGNOSTIC

La directive du 17 mai 2017 susmentionnée, dans le considérant 27 et l'annexe I, distingue désormais deux catégories d'armes qui étaient soumises à des régimes distincts : les armes historiques[29] et les reproductions d'armes historiques. Si les armes historiques restent exclues du champ de la directive, c'est-à-dire qu'elles demeurent libres d'acquisition et de détention, autant, désormais, leurs reproductions peuvent être réglementées.

Les reproductions d'armes à feu anciennes sont actuellement régies par les articles L. 311-3 et L. 311-4 du code de la sécurité intérieure. Ces articles soumettent les reproductions d'armes à feu anciennes à un régime identique à celui des armes à feu anciennes, à savoir à un principe de liberté d'acquisition et de détention. Du fait de ce régime de liberté, il n'existe pas de statistiques officielles ni même d'évaluations suffisamment fiables des armes de ce type détenues par les particuliers.

2. OBJECTIFS POURSUIVIS

La nouvelle directive part du constat que les reproductions d'armes à feu anciennes peuvent être construites en recourant aux techniques modernes susceptibles d'améliorer leur durabilité et leur précision. C'est la raison pour laquelle elle place ces armes dans son champ. L'objectif poursuivi par la directive est de dissocier le régime des armes historiques de celui de leurs reproductions, lorsque la technologie de ces dernières en renforce dangerosité.

Le classement des reproductions d'armes à feu anciennes en droit interne doit donc être modifié pour prendre en compte les armes qui ont pu bénéficier de techniques modernes susceptibles d'améliorer leur durabilité et leur précision.

---

[29] Selon, l'article L. 311-3 du code de la sécurité intérieure, les armes et matériels historiques et de collection ainsi que leurs reproductions sont :

1° Sauf lorsqu'elles présentent une dangerosité avérée, les armes dont le modèle est antérieur au 1er janvier 1900 ;

2° Les armes dont le modèle est postérieur au 1er janvier 1900 et qui sont énumérées par un arrêté conjoint des ministres de l'intérieur et de la défense compte tenu de leur intérêt culturel, historique ou scientifique ;

3° Les armes rendues inaptes au tir de toutes munitions, quels qu'en soient le modèle et l'année de fabrication, par l'application de procédés techniques et selon des modalités qui sont définis par arrêté conjoint des ministres de l'intérieur et de la défense, ainsi que des ministres chargés de l'industrie et des douanes.

Les chargeurs de ces armes doivent être rendus inaptes au tir dans les conditions fixées par l'arrêté prévu au premier alinéa du présent 3° ;

4° Les reproductions d'armes historiques et de collection dont le modèle est antérieur à la date prévue au 1°, sous réserve qu'elles ne tirent pas de munitions à étui métallique ;

5° Les matériels relevant de la catégorie A dont le modèle est antérieur au 1er janvier 1946 et dont la neutralisation est effectivement garantie par l'application de procédés techniques et selon les modalités définis par arrêté de l'autorité ministérielle compétente ;

6° Les matériels de guerre relevant de la catégorie A dont le modèle est postérieur au 1er janvier 1946, dont la neutralisation est garantie dans les conditions prévues au 5° et qui sont énumérés dans un arrêté du ministre de la défense compte tenu de leur intérêt culturel, historique ou scientifique.

3. NECESSITE DE LEGIFERER ET OPTION RETENUE

Les armes historiques et de collection ainsi que leurs reproductions sont actuellement classées par la loi en catégorie D (2° - armes dont l'acquisition et la détention sont libres).

Ce classement législatif constitue une anomalie juridique, puisque le classement relève du champ réglementaire. La transposition de la directive est l'occasion de revenir à un partage juridiquement plus exact du domaine législatif et du domaine réglementaire en la matière, en évitant ainsi la procédure de délégalisation, qui, au demeurant, n'était pas apparue nécessaire, puisque toutes ces armes (historiques et reproductions) étaient jusqu'alors soumises au même classement, ce qui n'est plus systématique aux termes de la directive.

Le choix est donc fait de revenir sur ce classement établi par la loi en modifiant l'article L. 311-4 du code de la sécurité intérieure.

4. ANALYSE DES IMPACTS DES DISPOSITIONS ENVISAGEES

4.1 Impact juridique

L'article L. 311-4 modifié par le présent projet de loi précise que les armes et matériels historiques et de collection, ainsi que leurs reproductions seront classés par décret en Conseil d'État. Certaines dispositions du code de la sécurité intérieure devront également être modifiées à cette occasion lorsqu'elles font référence à la catégorie D qui est supprimée par la directive du 17 mai 2017. Il en est ainsi notamment des articles L. 311-2, L. 312-3, L. 312-3-1, L. 312-4-2, L. 312-5, L. 312-11, L. 312-16, L. 314-2-1, L. 317-3-1, L. 317-3-2 et L. 317-4-1 du code de la sécurité intérieure et des articles L. 2331-1, L. 2339-4, et L. 2339-4-1 du code de la défense.

4.2 Impact économique

L'absence de données chiffrées sur le « parc » d'armes historiques et de leurs reproductions rend malaisée l'évaluation de l'impact économique de l'entrée des reproductions dans le champ de la directive. Si le régime de classement – réglementaire – reste relativement peu contraignant au plan administratif, l'impact devrait être faible.

4.3 Impact administratif

Seules les reproductions d'armes à feu anciennes construites en recourant aux techniques modernes susceptibles d'améliorer leur durabilité et leur précision seront concernées par ce nouveau régime, et par un classement par le ministre de l'intérieur. L'article R. 311-3 du code de la sécurité intérieure dispose en effet que les mesures de classement des armes dans les catégories définies à l'article R. 311-2, autres que celles prévues par arrêtés interministériels, sont prises par le ministre de l'intérieur, à l'exclusion de celles des matériels de guerre de la catégorie A2, prises par le ministre de la défense[30].

30 L'article R.311-3-1 du code de la sécurité intérieure précise que pour le classement des armes mentionnées au premier alinéa de l'article R. 311-3, le ministre de l'intérieur peut solliciter l'avis d'une commission de classement comprenant des représentants des ministères concernés. Un arrêté conjoint des ministres de la défense, de

Pour instruire ces décisions de classement, le ministre de l'intérieur peut solliciter l'avis d'experts techniques, au sein d'un réseau constitué, notamment, du banc national d'épreuve de Saint-Etienne, des laboratoires de police technique et scientifique de la direction générale de la police nationale et de la direction générale de la gendarmerie nationale. Le cas échéant, il peut également solliciter le concours d'un établissement technique désigné par le ministre de la défense, s'il s'agit d'armes susceptibles de présenter des caractéristiques techniques comparables à celles définies à la rubrique 2 du I de l'article R. 311-2[31].

Le ministre de l'intérieur peut enfin solliciter l'avis d'une commission de classement comprenant des représentants des ministères concernés[32].

5.1 Textes d'application

Le nouveau classement sera établi par décret en Conseil d'État en tenant compte des critères fixés par la directive (notamment modification de l'article R. 311-2 du code de la sécurité intérieure). Le texte d'application définira les modalités d'application de ces dispositions, ainsi que les modalités permettant aux détenteurs de ces armes de régulariser, le cas échéant, leurs situations au regard des nouveaux classements.

5.2 Application dans le temps

Le projet de loi portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité introduit des dispositions relatives à l'entrée en vigueur des différents articles du titre II, consacré à la transposition de la directive (UE) 2017/853 du Parlement européen et du Conseil du 17 mai 2017.

Il est prévu que les dispositions de l'article 14 entrent en vigueur à compter d'une date définie par décret en Conseil d'État et au plus tard le 14 septembre 2018.

Conformément aux dispositions de la directive (1 de l'article 2), ces modifications de classement devront intervenir au plus tard le 14 septembre 2018.

5.3 Application dans l'espace

Les dispositions du titre II de la présente loi s'appliquent sur l'ensemble du territoire de la République et notamment en Nouvelle-Calédonie, en Polynésie française, dans les îles Wallis-et-Futuna et dans les Terres australes et antarctiques françaises.

Conformément au principe de spécialité législative, les modifications des dispositions du livre III du code de la sécurité intérieure et du livre III de la 2ème partie du code de la défense, faites par le titre II de la présente loi, doivent être rendues expressément applicables aux collectivités et territoires susmentionnés. C'est l'objet des modifications prévues par les articles L. 344-1, L. 345-1, L. 346-1 et L. 347-1 du code de la sécurité intérieure et par les articles L. 2441-1, L. 2451-1, L. 2461-1 et L. 2471-1 du code de la défense.

---

l'intérieur, de la justice et des ministres chargés de l'industrie, du commerce, de la chasse, des douanes et des sports précise l'organisation et les modalités de fonctionnement de cette commission de classement. S'il s'avère que le matériel relève de la compétence du ministre de la défense, au titre de l'article R. 2332-1 du code de la défense, le ministre de l'intérieur lui transmet le dossier de classement dans les meilleurs délais.

31 Dernier alinéa de l'article R. 311-3 du code de la sécurité intérieure.

32 Article R. 311-3-1 du code de la sécurité intérieure.

LE SURCLASSEMENT DE CERTAINES ARMES EN CATÉGORIE A

1. ETAT DES LIEUX ET DIAGNOSTIC

La directive du 17 mai 2017[33] fixe des règles plus strictes pour les armes à feu les plus dangereuses) afin d'empêcher que leur acquisition, leur détention ou leur commerce soient autorisés, à de rares exceptions près dûment motivées.

La directive[34] autorise toutefois les États membres à déroger au nouveau régime d'interdiction d'acquisition et de détention des armes à feu, des parties essentielles et des munitions nouvellement classées en catégorie A pour certaines catégories de détenteurs, et, pour certains d'entre eux, sous certaines conditions exposés ci-après.

Certaines armes à feu semi-automatiques (d'une capacité supérieure à 10 coups pour les armes de poing et 20 coups pour les armes d'épaule classées en catégorie B conformément à l'article R. 311-2 du code de la sécurité intérieure[35]) qui étaient soumises à autorisation (catégorie B) seront désormais interdites à l'acquisition et à la détention pour les particuliers par l'effet de leur classement en catégorie A, sauf dérogation.

Le régime des dérogations ouvertes par la directive est le suivant :

1) en ce qui concerne les armes acquises avant le 13 juin 2017 :

Les détenteurs de telles armes acquises avant cette date pourront être autorisés à les conserver. Il s'agit là d'un choix laissé aux États membres par l'article 7§4 bis de la directive.

2) en ce qui concerne les armes acquises à compter du 13 juin 2017

2-1) armes nouvellement soumises au principe d'interdiction

Les armes semi-automatiques suivantes relève désormais du régime de l'interdiction :

- armes issues de la transformation d'une arme automatique (classées A6 selon la directive) ;
- armes à percussion centrale et à chargeur fixe pouvant contenir plus de 10 cartouches (armes longues) ou 20 cartouches (armes courtes) (classées A7 selon la directive) ;
- armes longues dont la longueur peut être réduite à moins de 60 cm après que la crosse ait été repliée ou enlevée sans l'aide d'outils (classées A8 selon la directive).

En revanche, les armes qui sont conçues pour recevoir un chargeur amovible pourraient continuer d'être soumises à autorisation (catégorie B). Seuls les chargeurs amovibles à grande

33 Articles 6 et 7, ainsi que la partie II de l'annexe I de la directive.

34 Articles 6 et 7 de la directive.

35 Armes issues de la transformation d'une arme automatique (classées A6 selon la directive) ;
- armes à percussion centrale et à chargeur fixe pouvant contenir plus de 10 cartouches (armes longues) ou 20 cartouches (armes courtes) (classées en A7 selon la directive) ;
- armes longues dont la longueur peut être réduite à moins de 60 cm après que la crosse ait été repliée ou enlevée sans l'aide d'outils (classées A8 selon la directive).

capacité (10 cartouches pour les armes longues ; 20 cartouches pour les armes courtes) seraient alors soumises au principe d'interdiction.

2-2) possibilités de déroger, pour certains détenteurs, au principe d'interdiction

- tireurs sportifs

Les tireurs sportifs pourront être autorisés à acquérir et à détenir des armes issues de la transformation d'une arme automatique, ainsi que des armes ou chargeurs à grande capacité. Les disciplines sportives recourant à ce type d'armes sont nombreuses et il est cohérent que les tireurs sportifs doivent pouvoir puissent continuer d'en bénéficier, puisque ce sont les détenteurs d'armes les plus strictement contrôlés en droit national, à la fois au plan de la pratique sportive, que de l'honorabilité et des conditions de sécurisation des armes détenues.

- collectionneurs

La directive, dans son article 6 alinéa 3, permet aussi aux États membres qui le souhaitent d'accorder exceptionnellement, dans des cas particuliers et dûment motivés, des autorisations à des collectionneurs d'armes d'acquérir et de détenir des armes de catégorie A, sous réserve du strict respect de conditions suffisantes de sécurité, notamment en termes de stockage. Les collectionneurs concernés doivent être identifiables dans les fichiers de données et tenir un registre des armes de catégorie A en leur possession.

Le droit national en vigueur en matière de collectionneurs résulte des articles L. 312-6-1 à L. 312-6-5 du code de la sécurité intérieure, qui ont introduit la possibilité d'acquérir et de détenir au titre de la collection des armes de la seule catégorie C, soumises à déclaration. Compte tenu de la dangerosité de ces armes, il n'a pas paru souhaitable d'étendre aux collectionneurs la dérogation prévue par la directive.

Autant, en effet, il est nécessaire de prendre en considération les armes aujourd'hui légalement détenues basculant en catégorie A (cas des tireurs sportifs et de certains services de sécurité), autant il n'a pas paru opportun d'étendre le bénéfice de cette dérogation à des personnes qui, aujourd'hui, n'ont déjà pas le droit de détenir de telles armes. C'est le cas des collectionneurs.

Il s'agit de limiter ainsi le nombre et le flux de ces armes, parmi les plus dangereuses compte tenu de leurs caractéristiques techniques.

- autres personnes

La directive, dans son article 6, permet enfin de maintenir un régime d'autorisation, « dans des cas particuliers, exceptionnels et dûment motivés », et « en vue de protéger la sécurité des infrastructures critiques, la navigation commerciale, les convois de grande valeur et les lieux sensibles, ainsi qu'à des fins de défense nationale, éducatives, culturelles, de recherche et historiques ».

Cette possibilité doit être interprétée comme permettant aux États membres de continuer à délivrer des autorisations d'acquisition et de détention d'armes de catégorie A à des personnes

exerçant certaines activités de sécurité privée, en justifiant toutefois le choix des activités retenues à ce titre.

Les services de sécurité privée détenant aujourd'hui ce type d'armes sont peu nombreux.

2. OBJECTIFS POURSUIVIS

La directive, en surclassant des armes qui étaient jusqu'alors classées en catégorie B, pour les soumettre à un régime de prohibition, a pour objectif de renforcer la sécurité publique, en considérant que les caractéristiques techniques de ces armes les rendent particulièrement dangereuses (mode d'approvisionnement semi-automatique, puissance de tir etc.).

3. NECESSITE DE LEGIFERER ET OPTIONS

Le choix a été fait par le projet de loi d'utiliser la possibilité de déroger au principe d'interdiction ouverte par la directive pour les disciplines sportives recourant à ce type d'armes et pour les services de sécurité privée autorisée. Comme indiqué précédemment, ce choix a été motivé par le fait que les tireurs sportifs sont les détenteurs d'armes les plus strictement contrôlés en droit national, à la fois au plan de la pratique sportive que de l'honorabilité et des conditions de sécurisation des armes détenues. Les autorisations permettant à certains services de sécurité d'acquérir et de détenir des armes de catégorie A seront encadrées par un décret en Conseil d'Etat,

Le projet de loi tire les conséquences du nouveau régime de surclassement des armes qui étaient jusqu'alors classées en catégorie B et dorénavant soumises au principe d'interdiction sauf dérogation.

4. ANALYSE DES IMPACTS DES DISPOSITIONS ENVISAGEES

4.1 Impact juridique

Il résulte, par le choix de la dérogation qui est fait, de soumettre désormais à un régime d'autorisation administrative préalable des armes qui sont, normalement, sous régime de prohibition. Cet impact est cependant relativement artificiel, puisque c'est le régime du surclassement combiné avec celui de la dérogation autorisée par la directive qui permet cette détention, et non pas un assouplissement *ex nihilo* du régime de détention.

Compte-tenu de ce qui précède, il convient donc de modifier en ce sens l'article L.312-2 du code de la sécurité intérieure, mais également, par coordination, tous les articles « L » faisant référence à cette détention – par exercice de la dérogation – d'armes de catégorie A : L 312-3, L312-3-1, L312-4, L312-4-3, L312-11, L.312-16 du même code.

4.2 Impact économique

Compte tenu du choix, par le projet de loi, du régime de la dérogation, dans le périmètre précisé ci-dessus, l'impact économique devrait être nul, puisque le flux d'armes achetées devrait rester constant.

5. MODALITÉS DE MISE EN ŒUVRE

5.1 Textes d'application

Un décret précisera, pour les deux catégories précitées (tireurs sportifs et services de sécurité privée), le champ et les modalités de la dérogation au principe d'interdiction d'acquisition et de détention. Il précisera également les modalités permettant aux détenteurs légaux de ces armes de régulariser leur situation au regard des nouveaux classements opérées conformément à la directive, dans le cadre de l'exercice des choix laissés aux États membres.

5.2 Application dans le temps

Une entrée en vigueur différée de ces dispositions est nécessaire. En effet, en cas d'entrée en vigueur de la loi dans les conditions de droit commun, les détenteurs légaux de ces armes nouvellement surclassées en catégorie A par la directive du 17 mai 2017 basculeraient dès publication de la loi dans un régime de détention illégale. Il est donc nécessaire pour des raisons de sécurité juridique de différer l'entrée en vigueur de ces nouvelles dispositions afin de permettre au pouvoir réglementaire de tirer les conséquences de cette modification législative et d'en aménager le régime juridique.

Le projet de loi prévoit que les dispositions envisagées entreraient en vigueur à compter d'une date définie par décret en Conseil d'Etat et au plus tard le 14 septembre 2018.

5.3 Application dans l'espace

Les dispositions de la présente loi s'appliqueraient sur l'ensemble du territoire de la République et notamment en Nouvelle-Calédonie, en Polynésie française, dans les îles Wallis-et-Futuna et dans les Terres australes et antarctiques françaises.

Conformément au principe de spécialité législative, les modifications des dispositions du livre III du code de la sécurité intérieure et du livre III de la 2ème partie du code de la défense, faites par le titre II de la présente loi, doivent être rendues expressément applicables aux collectivités et territoires susmentionnés. C'est l'objet des modifications prévues par les articles L. 344-1, L. 345-1, L. 346-1 et L. 347-1 du code de la sécurité intérieure et par les articles L. 2441-1, L. 2451-1, L. 2461-1 et L. 2471-1 du code de la défense.

L'INSTAURATION D'UN CONTRÔLE ADMINISTRATIF POUR LES COURTIERS D'ARMES DE CATÉGORIE C

1. ETAT DES LIEUX ET DIAGNOSTIC

La directive du 17 mai 2017 susmentionnée, dans son article 4 §3, soumet à réglementation la totalité des activités d'armuriers et de courtiers.

Selon le code de la sécurité intérieure, les armuriers sont désignés comme toute personne physique ou morale dont l'activité professionnelle consiste en tout ou en partie dans la fabrication, le commerce, l'échange, la location, la réparation ou la transformation d'armes, d'éléments essentiels et accessoires d'armes et de munitions (2° du III de l'article R. 311-1) tandis que les courtiers sont désignés comme les personnes physiques ou morales qui se livrent à une activité d'intermédiation (5° du III de l'article R. 311-1),

L'activité d'intermédiation (1° du III de l'article R. 311-1) correspondant à toute opération à caractère commercial ou à but lucratif dont l'objet est soit de rapprocher des personnes souhaitant conclure un contrat d'achat ou de vente de matériels de guerre, armes et munitions ou de matériels assimilés, soit de conclure un tel contrat pour le compte d'une des parties. Cette opération d'intermédiation faite au profit de toute personne quel que soit le lieu de son établissement prend la forme d'une opération de courtage ou celle d'une opération faisant l'objet d'un mandat particulier ou d'un contrat de commission

La directive prévoit que chaque État membre établit un système réglementant les activités des armuriers et des courtiers.

Cette réglementation doit comprendre, selon les termes de la directive, au moins les mesures suivantes:

- l'enregistrement des armuriers et des courtiers opérant sur le territoire de l'État membre ;
- l'obligation pour les armuriers et les courtiers d'être titulaires d'une licence ou d'une autorisation sur le territoire de l'État membre ;
- un contrôle de l'honorabilité professionnelle et privée et des compétences pertinentes de l'armurier ou du courtier concerné (s'il s'agit d'une personne morale, le contrôle porte sur la personne morale et sur la ou les personnes physiques qui dirigent l'entreprise).

Le code de la sécurité intérieure ne répond que partiellement à ces objectifs, puisque, si les armuriers sont tous soumis à contrôle administratif[36], quelles que soient les catégories d'armes

[36] Cf. l'article L. 313-2 du code de la sécurité intérieure qui prévoit que nul ne peut exercer à titre individuel l'activité qui consiste, à titre principal ou accessoire, en la fabrication, le commerce, l'échange, la location, la réparation ou la transformation d'armes, d'éléments d'armes et de munitions ni diriger ou gérer une personne morale exerçant cette activité s'il n'est titulaire d'un agrément relatif à son honorabilité et à ses compétences professionnelles, délivré par l'autorité administrative. Cet article concerne les armuriers pour les armes relevant des catégories C et D.

fabriquées ou commercialisées, seuls les courtiers, c'est-à-dire les acteurs économiques pratiquant l'intermédiation, exerçant dans le champ des armes de catégories B et A sont soumis à contrôle de l'État. Le I de l'article L. 2332-1 du code de la défense précise à cet égard que les entreprises de fabrication ou de commerce de matériels de guerre et d'armes et munitions de défense des catégories A ou B ne peuvent fonctionner et l'activité de leurs intermédiaires ou agents de publicité ne peut s'exercer qu'après autorisation de l'Etat et sous son contrôle.

2. OBJECTIFS POURSUIVIS

L'objectif poursuivi est, d'une part, d'assurer la transposition complète de la directive sur le contrôle des professionnels des armes, et, d'autre part, de combler une faille dans le dispositif national de contrôle de la circulation des armes civiles, en soumettant à un même contrôle tous les commerçants, depuis le fabricant jusqu'au vendeur détaillant en passant par les intermédiaires (courtiers). Ce contrôle porte sur l'honorabilité et les compétences professionnelles.

Il devra être différencié et adapté aux différents métiers du commerce des armes, pour garantir son efficience.

3. NECESSITE DE LEGIFERER ET OPTIONS

Pour assurer le complet respect de la directive, il est nécessaire de créer un contrôle des courtiers d'armes de catégorie C, qui ne sont pas contrôlés à ce jour.

La loi doit donc être modifiée à cette fin, pour soumettre ces courtiers, comme les armuriers, à contrôle d'honorabilité et de compétence professionnelle.

4. ANALYSE DES IMPACTS DES DISPOSITIONS ENVISAGEES

4.1 Impact juridique

L'article L. 313-2 du code de la sécurité intérieure modifié par le présent projet de loi précisera que nul ne peut exercer à titre individuel l'activité qui consiste, à titre principal ou accessoire, en la fabrication, le commerce, l'intermédiation, l'échange, la location, la location-vente, le prêt, la modification, la réparation ou la transformation d'armes, d'éléments d'armes et de munitions ni diriger ou gérer une personne morale exerçant cette activité s'il n'est titulaire d'un agrément relatif à son honorabilité et à ses compétences professionnelles, délivré par l'autorité administrative.

Le contrôle de l'honorabilité vise à s'assurer que le demandeur a un comportement compatible avec l'exercice de la profession envisagée, notamment en s'assurant que son casier judiciaire ne comporte pas de mention incompatible avec cette profession et au regard des préoccupations d'ordre et de sécurité publics. A cet égard, l'article R. 114-5 code de la sécurité intérieure précise que peuvent donner lieu aux enquêtes mentionnées à l'article R.

114-1 les autorisations ou agréments suivants relatifs à des matériels, produits ou activités présentant un danger pour la sécurité publique, notamment ceux relatifs à la fabrication, au commerce, à l'acquisition, à la détention, à l'importation et à l'exportation de matériels de guerre, armes et munitions.

Le contrôle des compétences professionnelles a pour objet de s'assurer que la personne concernée dispose d'une aptitude professionnelle adaptée à ce domaine d'activité[37].

4.2 Impact économique

Le nouveau régime de contrôle administratif ne devrait avoir, en tant que tel, aucun impact économique, sauf s'il apparaissait que certains opérateurs, aujourd'hui non contrôlés, ne répondraient pas aux exigences nouvelles en termes de compétence professionnelle et d'honorabilité, auquel cas ils ne pourraient plus continuer d'exercer l'activité.

On estime cependant que les opérateurs répondant à la définition du courtier sont très peu nombreux, s'agissant des armes de catégorie C. Le champ « naturel » de l'intermédiation est plus, en effet, le commerce des armes ou matériels de guerre des catégories A et B, déjà réglementée.

4.3 Impact social

Sous la même réserve que celle énoncée ci-dessus, ce nouveau régime n'aura aucun impact social.

4.4 Impact administratif

Ce nouveau régime nécessitera pour le ministère de l'intérieur d'instruire et de délivrer les titres administratifs autorisant l'exercice de cette profession, après contrôle d'honorabilité et des compétences professionnelles, selon un cahier des charges qui sera défini par voie réglementaire.

5. MODALITÉS DE MISE EN ŒUVRE

5.1 Textes d'application

Un décret en Conseil d'État fixera les modalités d'application de ce nouveau régime juridique applicable aux courtiers d'armes de catégorie C.

5.2 Application dans le temps

Les dispositions envisagées entreront quant à elles en vigueur au plus tard le 14 décembre 2019. Ces dispositions modifient l'article L. 313-2 du code de la sécurité intérieure afin de soumettre l'ensemble des courtiers d'armes de catégorie C à un contrôle portant sur leur honorabilité et leurs compétences professionnelles.

Le choix de la date du 14 décembre 2019 résulte du 2 de l'article 2 de la directive, qui laisse un délai supplémentaire aux États membres pour préciser, justement, ces conditions de

37 Cf. pour les armuriers, l'article R. 313-3 du code de la sécurité intérieure.

compétence professionnelle et d'honorabilité, et pour préparer à la bascule dans le nouveau régime de contrôle de ces courtiers.

5.3 Application dans l'espace

Les dispositions de la présente loi s'appliquent sur l'ensemble du territoire de la République et notamment en Nouvelle-Calédonie, en Polynésie française, dans les îles Wallis-et-Futuna et dans les Terres australes et antarctiques françaises.

Conformément au principe de spécialité législative, les modifications des dispositions du livre III du code de la sécurité intérieure et du livre III de la 2ème partie du code de la défense, faites par le titre II de la présente loi, doivent être rendues expressément applicables aux collectivités et territoires susmentionnés. C'est l'objet des modifications prévues par les articles L. 344-1, L. 345-1, L. 346-1 et L. 347-1 du code de la sécurité intérieure et par les articles L. 2441-1, L. 2451-1, L. 2461-1 et L. 2471-1 du code de la défense.

L'INTERDICTION DE LA LIVRAISON AU DOMICILE DE L'ACQUÉREUR DES ARMES ACHETÉES PAR CORRESPONDANCE

1. ETAT DES LIEUX ET DIAGNOSTIC

La directive du 17 mai 2017, dans son article 5 *ter*, ne modifie pas les règles des États membres qui permettent que les transactions sur des armes à feu, leurs parties essentielles et sur les munitions, soient faites au moyen de la vente par correspondance, sur internet ou au moyen des contrats à distance.

Toutefois, la directive exige que les droits nationaux organisent la vérification de l'identité des parties à ces transactions et leur légitimité à effectuer ces transactions et que ce contrôle soit effectif. C'est pourquoi, elle précise que, dans ce cas, la livraison d'armes à feu, leurs parties essentielles ou de munitions de la catégorie A, B ou C, doit faire l'objet d'une vérification de l'identité de l'acheteur et, le cas échéant, de son autorisation d'acquisition et de détention, avant la livraison ou au plus tard, au moment de la livraison. Cette vérification, selon la directive, doit être assurée soit auprès d'un armurier, soit auprès d'une autorité publique.

L'article L. 313-5 du code de la sécurité intérieure impose que les armes achetées à distance doivent être livrées chez un armurier. Cet article prévoit également une dérogation à cette obligation de livraison dans les locaux d'un armurier en renvoyant à un décret en Conseil d'État le soin de préciser le champ de cette dérogation.

Dans la pratique, la dérogation est ouverte à toutes les catégories d'armes sans distinction. En effet, l'article R. 313-23 du code de la sécurité intérieure dispose qu'en application de l'article L. 313-5 du même code, les armes et leurs éléments des catégories B, C, du 1° et des g et h du 2° de la catégorie D et les munitions de toute catégorie peuvent, par dérogation à l'article L. 313-4, être livrés directement à l'acquéreur dans le cadre d'une vente par correspondance ou à distance, dans le respect des dispositions du chapitre V.

Ces régimes de dérogation reposent sur un contrôle de l'identité de l'acheteur qui ne fait l'objet d'aucune vérification préalable ou concomitante à la livraison par une autorité publique ou par un armurier, lorsque la transaction est faite de particulier à particulier. Même pour les armes de catégorie B cédées par un particulier à un autre particulier, ce contrôle n'est pas obligatoire, préalablement à la transaction,

L'acheteur n'est en effet tenu que d'envoyer au vendeur une photocopie d'un document d'identité, ce qui n'offre aucune garantie d'authenticité et ne respecte pas les dispositions nouvelles de la directive.

Le fait de vendre ou d'acheter des matériels de guerre, des armes, des munitions ou leurs éléments en méconnaissance des dispositions de l'article L. 313-5 constitue un délit passible de cinq ans d'emprisonnement et de 75 000 euros d'amende.

2. OBJECTIFS POURSUIVIS

Le présent projet de loi prévoit d'imposer une vérification de l'identité de l'acheteur et, le cas échéant, de son autorisation d'acquisition et de détention, avant la livraison ou au plus tard, au moment de la livraison, soit auprès d'un armurier, soit auprès d'une autorité publique. Ce nouveau régime doit permettre de renforcer la sécurité publique en évitant que des transactions bénéficient à des personnes non autorisées ou qui souhaiteraient se soustraire au contrôle administratif.

Le projet de loi a pour objectif de supprimer la dérogation actuellement autorisée dans le droit national s'agissant des ventes entre particuliers.

3. NECESSITE DE LEGIFERER ET OPTIONS

En opportunité, il a été estimé qu'il fallait, d'une part, empêcher toute possibilité de dérogation pour ces ventes entre particuliers, en neutralisant toute demande d'assouplissement au principe de l'interdiction par voie réglementaire. D'autre part, il est également apparu nécessaire de garantir le plein effet de la directive en limitant, législativement, le champ des dérogations à l'interdiction de livraison au domicile.

Il est de ce fait proposé de supprimer toute possibilité de déroger à la livraison obligatoire dans des locaux d'armuriers.

La directive ouvre aux Etats la possibilité de faire contrôler ces livraisons d'armes, soit par les armuriers ou courtiers, soit par une autorité publique. Celle-ci ne pourrait être, en France, que les services de police ou de gendarmerie, ou les services des préfectures.

Il n'a pas paru opportun au Gouvernement de solliciter les commissariats de police ou les brigades de gendarmerie ni les services des préfectures pour ne pas créer des charges de gestion nouvelles pour les services de l'État.

Le passage par l'armurier garantit de son côté un contrôle qu'il est mieux à même d'effectuer, s'agissant de la nature de l'arme qu'il recevra (son classement, et donc l'adéquation du titre de détention par rapport au classement de l'arme), avant sa livraison à l'acquéreur.

Cette vérification exige une compétence technique (professionnelle) dont l'armurier est garant, plus encore que les services de l'État.

4. ANALYSE DES IMPACTS DES DISPOSITIONS ENVISAGEES

4.1 Impact juridique

Il est proposé de modifier l'article L. 313-5 du code de la sécurité intérieure afin d'être en conformité avec les objectifs de la directive. L'interdiction prévue nécessite de modifier l'article L. 313-5 du code de la sécurité intérieure, qui définit aujourd'hui le régime des ventes à distances d'armes et des munitions, et ouvre sans limitation aucune, la possibilité de déroger à l'interdiction de livraison à domicile.

4.2 Impact économique

Le nouveau régime pourrait avoir un impact économique dans les relations entre particuliers, si l'obligation de réaliser la transaction sous le contrôle d'un armurier devait freiner ces transactions. Il s'agit cependant, en tout état de cause, de flux financiers modestes, sans effet notable sur les équilibres économiques.

S'agissant des armuriers, la prohibition de la livraison à domicile des armes vendues entre particuliers pourrait engendrer des frais ou des contraintes de gestion (réception des armes, stockage éventuel pendant quelques jours, temps passé à contrôler la transaction – identité de l'acquéreur, existence d'un éventuel titre de détention, contrôle du fichier des interdits de détention d'armes -). Ces frais et ces contraintes devraient être répercutés sur les parties à la vente, sous forme d'une commission qu'il appartiendra à l'armurier de fixer librement. Il n'a pas paru souhaitable, en effet, que l'État intervienne dans la détermination de la tarification d'une prestation commerciale, qui pourra être variable, au demeurant, si l'armurier se limite aux vérifications réglementaires, ou s'il propose à l'acquéreur, en outre, une prestation qui s'approcherait d'un contrôle technique, ce que rien n'interdit mais qui ne sera pas obligatoire non plus.

4.3 Impact administratif

A partir du moment où la livraison des armes vendues à distance de particulier à particulier se ferait chez les professionnels, les mesures envisagées ne devraient avoir aucun impact sur les services de l'État lesquels ne seront pas mis à contribution pour contrôler ces ventes.

5. MODALITÉS DE MISE EN ŒUVRE

5.1 Textes d'application

Un décret en Conseil d'État précisera les modalités d'application des présentes dispositions, notamment afin de supprimer la dérogation à l'obligation de se faire livrer les armes, les munitions et leurs éléments essentiels dans une armurerie pour les particuliers et de préciser les modalités du contrôle de l'identité et des titres de détention produits à l'occasion de cette vente.

5.2 Application dans le temps

Des dispositions transitoires et d'entrée en vigueur différée sont indispensables pour ces dispositions afin d'éviter un effet couperet dès l'entrée en vigueur de la présente loi. Cette entrée en vigueur différée est calée sur la date de transposition générale de la directive, soit le 14 septembre 2018. S'agissant d'une mesure ayant pour objet principal la protection de l'ordre et de la sécurité publics, il n'a pas paru opportun d'aller au-delà de cette date.

5.3 Application dans l'espace

Les dispositions de la présente loi s'appliquent sur l'ensemble du territoire de la République notamment en Nouvelle-Calédonie, en Polynésie française, dans les îles Wallis-et-Futuna et dans les Terres australes et antarctiques françaises.

Conformément au principe de spécialité législative, les modifications des dispositions du livre III du code de la sécurité intérieure et du livre III de la 2ème partie du code de la défense, faites par le titre II de la présente loi, doivent être rendues expressément applicables aux collectivités et territoires susmentionnés. C'est l'objet des modifications prévues par les articles L. 344-1, L. 345-1, L. 346-1 et L. 347-1 du code de la sécurité intérieure et par les articles L. 2441-1, L. 2451-1, L. 2461-1 et L. 2471-1 du code de la défense. .

LES TRANSACTIONS SUSPECTES

1. ETAT DES LIEUX ET DIAGNOSTIC

La directive, dans son article 10§2, prévoit la possibilité, pour les armuriers, de refuser légalement des transactions portant sur des munitions et composants de munitions qui apparaîtraient comme suspectes en raison de leur nature ou de leur échelle.

Elle prévoit aussi un régime de signalement de ces tentatives de transaction. Il s'agit, en droit, d'une dérogation à un principe du droit de la consommation (refus de vente ou de prestation). En effet, en droit interne, l'article L. 121-11 (alinéa 1er) du code de la consommation précise qu'est interdit le fait de refuser à un consommateur la vente d'un produit ou la prestation d'un service, sauf motif légitime. Ce principe est sanctionné par l'article R. 132-1 du même code qui prévoit que les refus de vente ou de prestation de services, en méconnaissance des dispositions du premier alinéa de l'article L. 121-11, sont punis de la peine d'amende prévue pour les contraventions de la 5e classe.

C'est donc par une dérogation légale à la réglementation sur le refus de vente qu'est instituée cette possibilité de refuser les transactions suspectes conformément aux objectifs fixées par la directive du 17 mai 2017[38].

2. OBJECTIFS POURSUIVIS

Dans un souci de sécurité publique, le projet de loi prévoit de permettre aux armuriers et aux courtiers de refuser de conclure toute transaction visant à acquérir des armes, cartouches complètes de munitions, ou de composants de munitions, qu'ils pourraient raisonnablement considérer comme suspecte, en raison de sa nature ou de son échelle, et de signaler toute tentative de transaction de ce type aux autorités compétentes.

3. NECESSITE DE LEGIFERER ET OPTIONS

L'article 10§2 de la directive ne vise que les transactions relatives à des cartouches complètes de munitions ou d'éléments de munitions. La transposition de la directive ne s'oppose toutefois pas à une mise en cohérence de la législation française puisqu'elle autorise les Etats membres à prévoir des mesures plus contraignantes en droit interne. Le gouvernement a saisi cette opportunité pour étendre la faculté offerte aux armuriers aux armes et aux éléments d'armes.

En l'absence de dispositions dans le code de la sécurité intérieure, il convient de compléter ce code par un article L. 313-6.

38 Cf. également la réglementation sur les précurseurs d'explosifs : décret n° 2017-1308 du 29 août 2017 relatif à la commercialisation et à l'utilisation de précurseurs d'explosifs.

4. ANALYSE DES IMPACTS.

4.1 Impact juridique

L'article L. 313-6 qu'il est proposé d'ajouter au code de la sécurité intérieure aura pour impact juridique, non pas de contraindre les armuriers à refuser toute transaction sur laquelle ils pourraient avoir un doute, mais de les mettre à l'abri de toutes poursuites pénales, s'ils refusent une telle vente (au regard de la qualification pénale de refus de vendre).

Ainsi l'armurier ou le courtier ne sera pas dans l'obligation de refuser systématiquement de conclure la transaction en présence d'un doute. Il devra en revanche signaler la tentative de transaction suspecte en cas de refus de sa part.

Le caractère suspect d'une transaction est en effet subjectif, raison pour laquelle il est difficile d'établir une incrimination. Si une transaction manifestement suspecte ne fait pas l'objet d'un refus, l'armurier pourrait être inquiété, le cas échéant, dans le cadre d'une procédure pénale, notamment par application des règles relatives à la complicité (par aide et assistance).

Le seul cas pouvant objectivement donner lieu à incrimination est celui du refus de transaction suspecte qui ne ferait pas l'objet d'un signalement, cas dans lequel le pouvoir réglementaire pourra prévoir une contravention de cinquième classe.

En outre, en plus des éventuelles sanctions pénales, des sanctions administratives sont susceptibles d'être encourues. A titre d'illustration, l'article R. 313-7 du code de la sécurité intérieure prévoit la possibilité de suspendre ou de retirer, pour des raisons d'ordre public et de sécurité des personnes, l'agrément d'armurier.

Le 2° de l'article R. 313-18 du même code prévoit la possibilité de suspendre ou de retirer l'autorisation d'ouverture de local commercial de l'armurier lorsque ne sont plus remplies les conditions auxquelles cette autorisation est soumise lors de sa délivrance, notamment lorsque l'exploitation du local est à l'origine de troubles répétés à l'ordre ou à la sécurité publics.

Enfin, le II de l'article R. 313-38 de ce code prévoit la possibilité de retirer l'autorisation de fabrication et de commerce pour des raisons d'ordre ou de sécurité publics.

4.2 Impact économique

Les transactions suspectes sont exceptionnelles : l'impact économique est donc nul, surtout mis en balance avec l'impact positif en termes de sécurité publique. En effet, en pratique, la majorité des transactions suspectes a lieu hors réseau des armuriers et du commerce licite.

5. MODALITÉS DE MISE EN ŒUVRE

5.1 Textes d'application

Un décret en Conseil d'Etat fixera les modalités d'application des dispositions relatives à la transaction suspecte.

5.2 Application dans le temps

Des dispositions transitoires et d'entrée en vigueur différée sont indispensables pour ces dispositions afin de préciser le nouveau dispositif, notamment le point de contact pour les signalements de transactions suspectes. Cette entrée en vigueur différée est alignée sur la date de transposition générale de la directive, soit le 14 septembre 2018, s'agissant d'une mesure ayant pour objet principal la protection de l'ordre et de la sécurité publics.

5.3 Application dans l'espace

Les dispositions de la présente loi s'appliquent sur l'ensemble du territoire de la République notamment en Nouvelle-Calédonie, en Polynésie française, dans les îles Wallis-et-Futuna et dans les Terres australes et antarctiques françaises.

Conformément au principe de spécialité législative, les modifications des dispositions du livre III du code de la sécurité intérieure et du livre III de la 2ème partie du code de la défense, faites par le titre II de la présente loi, doivent être rendues expressément applicables aux collectivités et territoires susmentionnés. C'est l'objet des modifications prévues par les articles L. 344-1, L. 345-1, L. 346-1 et L. 347-1 du code de la sécurité intérieure et par les articles L. 2441-1, L. 2451-1, L. 2461-1 et L. 2471-1 du code de la défense.

TITRE III - MISE EN ŒUVRE DE LA DÉCISION N° 1104/2011/UE DU PARLEMENT EUROPÉEN ET DU CONSEIL DU 25 OCTOBRE 2011 RELATIVE AUX MODALITÉS D'ACCÈS AU SERVICE PUBLIC RÉGLEMENTÉ OFFERT PAR LE SYSTÈME MONDIAL DE RADIONAVIGATION PAR SATELLITE ISSU DU PROGRAMME GALILEO

1. ETAT DES LIEUX ET DIAGNOSTIC

1.1 Contexte

Le programme Galileo, initié en 1999, vise à mettre en place et à exploiter une infrastructure de radionavigation et de positionnement par satellite spécifiquement conçue à des fins civiles, qui peut être utilisée par une multitude d'acteurs publics et privés en Europe et dans le monde. L'infrastructure comprend des satellites et un réseau de stations au sol. Le système issu du programme Galileo fonctionne indépendamment des autres systèmes comparables (*Global positioning system* - GPS, Glonass[39], *Beidou*[40], etc.) et contribue ainsi à assurer l'autonomie stratégique de l'Union européenne. Il offre des fonctionnalités beaucoup plus étendues que le programme européen EGNOS, qui vise à améliorer la qualité des signaux du système américain GPS et du système russe *Glonass* dans le but d'en assurer la fiabilité sur une vaste zone géographique.

La gestion du programme Galileo de radionavigation par satellite est entrée, au début 2001, dans sa phase de développement, qui visait à vérifier et à tester les hypothèses retenues pendant la phase de définition, notamment quant aux différentes composantes de l'architecture du système. Cette phase est suivie par la phase actuelle du déploiement, qui consiste à fabriquer des satellites et des composantes terrestres, à lancer des satellites et à installer des stations et des équipements terrestres afin que le système puisse être pleinement opérationnel.

Initialement construit comme un partenariat entre financements publics et privés (*Galileo Joint Undertaking*), le programme Galileo fait l'objet depuis 2007 d'une maîtrise assurée par la Commission Européenne : ainsi, l'agence du GNSS européen (GSA) créée en 2004 a repris en 2007 l'ensemble des activités de l'entreprise commune Galileo qui a été dissoute.

Les premiers lancements ont eu lieu en 2011.

À ce stade, dix-huit des trente satellites prévus ont été lancés. La phase de capacité opérationnelle initiale a été déclarée le 15 décembre 2016, et la capacité opérationnelle complète est attendue pour 2020. La constellation de trente satellites (dont vingt-quatre en fonction et six satellites supplémentaires, pouvant servir de secours) devrait être en orbite en 2021.

Le coût une fois le programme Galileo déployé est évalué à une dizaine de milliards d'euros[41]. La France contribue pour près d'un cinquième aux budgets des programmes spatiaux européens. Le marché mondial des produits et des services liés à la mise en place de la

[39] Système global de navigation satellitaire russe.
[40] Système global de navigation satellitaire chinois.
[41] Référé de la Cour des comptes, publié le 26 janvier 2016 : https://www.ccomptes.fr/fr/documents/31431.

radionavigation par satellite est en forte expansion (+ 30 % par an selon la Commission européenne[42]). Il est estimé que 6 à 7 % du PIB de l'Union dépendent de la navigation par satellite[43]. En plus des applications de géolocalisation, la radionavigation par satellite permet, entre autres, la synchronisation de réseaux essentiels à l'économie (communication, transport d'électricité, transmission de données, etc.).

Outre le service ouvert, accessible à tous, et un service commercial, plus précis mais dont l'utilisation sera payante, le programme Galileo offre un troisième service, dénommé service public réglementé (SPR), parfois aussi désigné par le sigle anglais PRS (*public regulated service*). Le SPR est réservé aux seuls utilisateurs autorisés par les gouvernements, pour les applications sensibles qui exigent un contrôle d'accès efficace et un niveau élevé de continuité du service, même dans les situations de crise les plus graves. Il est adapté aux services qui exigent une robustesse et une fiabilité absolue. Son signal sécurisé offre une protection supplémentaire contre les tentatives de brouillage ou de leurrage.

1.2 Etat du droit

Le droit français ne comporte actuellement aucune disposition relative au service public réglementé de Galileo. À ce stade, la seule marque du programme Galileo sur le droit français résulte du décret n° 2014-1507 du 15 décembre 2014 portant publication de l'accord relatif signé à Paris le 12 juin 2013, dont l'approbation a été autorisée par la loi n° 2014-548 du 28 mai 2014. Ces stipulations sont relatives à l'hébergement et au fonctionnement du centre de sécurité Galileo, et ne comportent pas de normes relatives au service public réglementé de Galileo.

La décision n° 1104/2011/UE du Parlement européen et du Conseil du 25 octobre 2011 publiée au Journal officiel de l'Union européenne le 4 novembre 2011 précise les obligations des Etats membres qui souhaitent recourir au service public réglementé offert par le système mondial de radionavigation par satellite issu du programme Galileo, au nombre desquels se trouve la France, en vue d'assurer leur propre sécurité, et la sécurité de l'Union. Cette décision requiert que l'accès au SPR soit strictement restreint à certaines catégories d'utilisateurs faisant l'objet d'un contrôle permanent, assuré par une « autorité responsable du service public réglementé », fonction qui est dévolue, pour la France, au secrétariat général de la défense et de la sécurité nationale (SGDSN).

La décision n° 1104/2011/UE prend place dans le cadre plus large de la mise en place et de l'exploitation des systèmes européens de radionavigation par satellite, qui sont régis par le règlement (UE) n° 1285/2013 du Parlement européen et du Conseil, qui a remplacé les anciens règlements (CE) n° 876/2002, qui initiait la phase de développement du programme Galileo, et n° 683/2008, qui était relatif à la poursuite de la mise en œuvre des programmes européens de radionavigation par satellite.

La décision n° 1104/2011/UE susmentionnée ne fixe pas d'échéance pour sa mise en œuvre en droit national, si ce n'est le 6 novembre 2013 pour la désignation d'une autorité responsable du

[42] *Ibidem.*
[43] *Ibidem*

service public réglementé[44]. Toutefois, la mise en œuvre des obligations qu'elle fixe est une condition pour pouvoir bénéficier du service public réglementé, et constitue donc une incitation à adopter les normes nationales nécessaires à cette fin.

La décision n° 1104/2011/UE prévoit que les règles relatives à l'accès au SPR, à la fabrication et au développement des récepteurs SPR et des modules de sécurité associés, et à l'exportation des équipements, de technologie et de logiciels relatifs au SPR sont précisées par des normes minimales communes, dont les domaines sont énumérés en annexe de ladite décision. Ces normes minimales communes ont été adoptées par une décision déléguée (de référence C(2015) 612 final, dont les Etats membres ont été rendus destinataires) de la Commission du 15 septembre 2015, complétant la décision n° 1104/2011/UE.

2. OBJECTIFS POURSUIVIS

Le tableau suivant synthétise les principales dispositions de la décision n° 1104/2011/UE qui appellent à prendre des mesures de transposition:

Article 3	Article 3.3 : Chaque État membre qui a recours au PRS décide de manière indépendante, d'une part, des catégories de personnes physiques résidant sur son territoire ou exerçant des fonctions officielles à l'étranger au nom de cet État membre et des catégories de personnes morales établies sur son territoire qui sont autorisées à être des utilisateurs du PRS et, d'autre part, des utilisations qui en sont faites, conformément à l'article 8 (normes minimales communes). Ces utilisations peuvent comprendre des utilisations liées à la sécurité.
Article 5	Article 5.4 : Chaque autorité PRS responsable veille à ce que l'utilisation du PRS soit conforme à l'article 8 (normes minimales communes).
	Article 5.5 : L'autorité PRS responsable d'un État membre veille à ce qu'une entité établie sur le territoire de cet État membre ne puisse développer ou fabriquer des récepteurs PRS ou des modules de sécurité que si cette entité : a) a été dûment autorisée par le conseil d'homologation de sécurité conformément à l'article 11, paragraphe 2, du règlement (UE) n° 912/2010 ; et b) se conforme à la fois aux décisions du conseil d'homologation de sécurité, à l'article 8 (normes minimales communes) pour ce qui concerne le développement et la fabrication des récepteurs PRS ou des modules de sécurité, dans la mesure où ces dispositions portent sur ses activités. Toute autorisation prévue au présent paragraphe aux fins de la fabrication d'équipements fait l'objet d'un réexamen au moins tous les cinq ans.

[44] En France, le secrétariat général de la défense et de la sécurité nationale.

	Article 5.6 : S'agissant des activités de développement ou de fabrication visées au paragraphe 5 du présent article, ou dans le cas d'exportations en dehors de l'Union, l'autorité PRS responsable de l'État membre concerné joue le rôle d'interface pour les entités compétentes en matière de restrictions à l'exportation des équipements, de la technologie et des logiciels pertinents en ce qui concerne l'utilisation et le développement du PRS et la fabrication destinée à celui-ci, afin de garantir l'application des dispositions de l'article 9.
Article 7	Article 7.1 : Un État membre peut, sous réserve des exigences énoncées à l'article 5, paragraphe 5, confier à des entités établies sur son territoire ou sur le territoire d'un autre État membre la fabrication des récepteurs PRS ou des modules de sécurité associés.
Article 8	1. Les normes minimales communes auxquelles doivent se conformer les autorités PRS responsables visées à l'article 5 portent sur les domaines énumérés à l'annexe. 2. La Commission est habilitée à adopter des actes délégués en conformité avec l'article 11 en ce qui concerne l'adoption des normes minimales communes dans les domaines énumérés à l'annexe et, le cas échéant, des modifications actualisant l'annexe pour tenir compte de l'évolution du programme Galileo, notamment sur le plan de la technologie, et des modifications des besoins en matière de sécurité.
Article 9	Les exportations, en dehors de l'Union, d'équipements, de technologie ou de logiciels relatifs à l'utilisation et au développement du PRS et à la fabrication destinée à celui-ci ne sont autorisées que conformément à l'article 8 et au point 3 de l'annexe et au titre des accords visés à l'article 3, paragraphe 5, ou au titre des accords concernant les modalités d'hébergement et de fonctionnement des stations de référence.
Article 10	La présente décision est appliquée sans préjudice des mesures arrêtées en vertu de l'action commune 2004/552/PESC.
Article 15	Les États membres déterminent le régime des sanctions applicables aux violations des dispositions nationales adoptées en application de la présente décision. Les sanctions sont efficaces, proportionnées et dissuasives.

3. OPTIONS ET NECESSITE DE LEGIFERER

La décision n° 1104/2011/UE du Parlement européen et du Conseil susmentionnée constitue un acte législatif pris, selon la procédure législative ordinaire, sur la base de l'article 172 du traité sur le fonctionnement de l'Union européenne (TFUE).

Cet article 172 TFUE s'inscrit dans le titre XVI dudit traité, qui est relatif aux réseaux transeuropéens - « l'Union contribue à l'établissement et au développement de réseaux transeuropéens dans les secteurs des infrastructures du transport, des télécommunications et de l'énergie » (article 170 du TFUE) ; ce titre s'inscrivant dans la 3ème partie du Traité consacrée aux « politiques et actions internes de l'union ».

Aux termes de l'article 171 du TFUE : « 1. Afin de réaliser les objectifs visés à l'article 170, l'Union :

- établit un ensemble d'orientations couvrant les objectifs, les priorités ainsi que les grandes lignes des actions envisagées dans le domaine des réseaux transeuropéens ; ces orientations identifient des projets d'intérêt commun ;
- met en œuvre toute action qui peut s'avérer nécessaire pour assurer l'interopérabilité des réseaux, en particulier dans le domaine de l'harmonisation des normes techniques (…) ».

Les orientations et les autres mesures visées à l'article 171, paragraphe 1, sont arrêtées par le Parlement européen et le Conseil, statuant conformément à la procédure législative ordinaire et après consultation du Comité économique et social et du Comité des régions (article 172 du TFUE).

La décision n° 1104/2011/UE est donc une mesure visée à l'article 171 paragraphe 1, arrêtée conformément à l'article 172 sous la forme d'une décision, obligatoire dans tous ses éléments (article 288 du TFUE), adoptée selon la procédure législative ordinaire (articles 289 §1 et 294 du TFUE).Elle s'inscrit dans la ligne de l'ancien règlement (CE) n° 683/2008 du Parlement européen et du Conseil du 9 juillet 2008 relatif à la poursuite de la mise en œuvre des programmes européens de radionavigation par satellite (EGNOS et Galileo), lui-même pris sur la base des dispositions du titre du Traité instituant la Communauté européenne (TCE) consacré aux réseaux transeuropéens.

Aux termes de l'article 1er du Règlement n° 683/2008 précité : « 4. Les objectifs spécifiques des programmes figurent en annexe. », et cette annexe prévoit que « Les objectifs spécifiques du programme Galileo consistent à assurer que les signaux émis par le système peuvent être utilisés pour exercer les cinq fonctions suivantes: (…) offrir un « service public réglementé» (dit « *Public Regulated Service* » ou PRS) réservé aux utilisateurs autorisés par les gouvernements, pour les applications sensibles qui exigent un niveau élevé de continuité du service. Le «service public réglementé» utilise des signaux robustes et cryptés (…) ».

Le respect des obligations fixées par la décision n° 1104/2011/UE nécessite de recourir à la loi, à deux titres.

En premier lieu, le SPR n'étant accessible qu'aux utilisateurs autorisés par les gouvernements, la mise en place du régime d'autorisation qui en découle nécessite l'intervention de la loi, qui doit couvrir les trois domaines requis :

- l'utilisation du SPR,
- la fabrication et le développement des récepteurs SPR et des modules de sécurité associés,
- l'exportation des équipements, de technologie et de logiciels relatifs au SPR.

Ce dispositif permettra à l'autorité administrative d'assurer le respect des normes minimales communes énumérées en annexe de la décision, en termes, notamment, d'organisation des groupes d'utilisateurs, de définition de la gestion de leurs droits d'accès, de distribution des

clés du service public réglementé et des informations classifiées y afférentes, de gestion de la sécurité.

Afin de permettre la vérification requise par les normes minimales communes pour les transferts intra-communautaires d'équipements, de technologie et de logiciels relatifs au SPR, une déclaration sera requise pour ces transferts.

En second lieu, la décision n° 1104/2011/UE requiert l'adoption de sanctions efficaces, proportionnées et dissuasives. Compte tenu de la sensibilité des applications du service public réglementé et des enjeux de sécurité associés il apparaît que des sanctions pénales (détaillées ci-après) sont adaptées. L'intervention de la loi est nécessaire, conformément à l'article 34 de la Constitution, pour déterminer les infractions, à caractère délictuel, aux règles de protection du service public réglementé, ainsi que les peines qui leur sont applicables.

4. ANALYSE DES IMPACTS DES DISPOSITIONS ENVISAGEES

4.1 Impact juridique

Le projet de loi, qui introduit dans le titre II du livre III de la partie 2 du code de la défense un chapitre consacré service public réglementé offert par le système mondial de radionavigation par satellite issu du programme européen Galileo, ne modifie pas de dispositions existantes. Conformément aux obligations découlant de la décision n° 1104/2011/UE, il instaure un régime d'autorisation préalable tant pour l'accès à ce service, que pour le développement et la fabrication de récepteurs et modules de sécurité et enfin l'exportation, hors du territoire de l'Union européenne, des équipements, technologies et logiciels relatifs à ce service.

Les équipements, technologie ou logiciels en cause pouvant cependant relever de catégories de biens dont l'exportation est soumise à autorisation en vertu d'autres régimes prévus par la législation nationale ou européenne (matériels de guerre, armes et munitions d'une part, biens à double usage d'autre part), le projet précise que l'autorisation préalable est délivrée sans préjudice de l'application :

- des dispositions du code de la défense applicables aux importations et exportations des matériels de guerre (articles L. 2335-1 et suivant du code de la défense) ;
- du règlement n° 428/2009 du Conseil du 5 mai 2009 instituant un régime communautaire de contrôle des exportations, des transferts, du courtage et du transit de biens à double usage qui en régissent l'exportation, dont les conditions d'application sont déterminées par le décret n° 2001-1192 du 13 décembre 2001 relatif au contrôle à l'exportation, à l'importation et au transfert de biens et technologies à double usage.

Les transferts au sein de l'Union européenne d'équipements conçus pour l'utilisation du service seront quant à eux soumis au seul régime de déclaration.

Enfin les sanctions pénales dont est assorti le dispositif visent à être proportionnées et dissuasives, ainsi que l'exige la décision transposée, tant pour les entreprises de taille moyenne que pour des acteurs économiques plus importants. Il est prévu de faire du défaut

d’autorisation ou du non-respect des conditions ou restrictions dont est assortie l’autorisation un délit, de même que la tentative, punis d’une amende de 200 000 euros. Quant au défaut de déclaration, pour les transferts intra-communautaires, il est prévu de le punir d’une amende de 50 000 euros. Des peines complémentaires sont également prévues, tant pour les personnes morales que pour les personnes physiques. Ces montants apparaissent proportionnés et dissuasifs, en particulier pour les personnes physiques. S’agissant des personnes morales de plus grande taille, telles que les industriels de la défense, les peines complémentaires également encourues permettront d’atteindre ce même objectif, notamment par la fermeture d’un ou plusieurs établissements ou l’exclusion temporaire des marchés publics.

4.2 Impact économique

Le projet de loi impose de nouvelles obligations aux seuls utilisateurs, fabricants et exportateurs de biens et services liés au service public réglementé de Galileo. Le coût de ces obligations ne pèsera néanmoins que sur les personnes intéressées par les fonctionnalités offertes par le service et bénéficiaires de l’autorisation. À ce jour, il est estimé que seront concernés quelques dizaines d’industriels, s’agissant de la fabrication, du développement et de l’exportation, et d’une dizaine à quelques dizaines de communautés utilisatrices. Pour ces entités, la charge administrative est comparable à celle d’un processus de certification, chacune d’elles devant justifier satisfaire entre vingt et trente critères techniques.

A ce stade, sont identifiés principalement des communautés d'utilisateurs relevant des ministères régaliens (défense, affaires étrangères, intérieur, justice) et des acteurs industriels impliqués dans le développement et la fabrication des récepteurs et modules de sécurité. Cette utilisation pourra progressivement s’étendre aux infrastructures critiques de transport, d’énergie ou de télécommunication.

L’impact de ces obligations nouvelles doit être mis en balance avec, d'une part, les bénéfices retirés du droit d'accéder au SPR pour les utilisateurs (continuité et robustesse du service, protection renforcée contre le brouillage et le leurrage) et pour les industriels (nouvelles opportunités de développement économique) concernés, et d'autre part avec le coût pour la France et pour l'Union européenne dans son ensemble qu'auraient des atteintes et des menaces dirigées contre l'intégrité de ce service. Cette préoccupation est telle, compte tenu de l'importance stratégique du programme Galileo en général et du SPR en particulier, que la décision n° 2014/496/PESC du Conseil du 22 juillet 2014 a prévu les modalités de réponse spécifiques, y compris en urgence, à des menaces ou à des atteintes de cette nature. Ces réponses pourraient aller jusqu'à des suspensions ou cessations d'autorisations accordées, afin d'assurer la protection même du service public réglementé, si des compromissions ou des vulnérabilités critiques venaient à être identifiées.

4.3 Impact social

Le cadre légal proposé vise à garantir la disponibilité d'un service sécurisé de radionavigation, de positionnement et de synchronisation y compris en cas de crise grave. Il contribuera ainsi à assurer la continuité d'activités économiques et sociales de la nation, et au développement de

nouvelles solutions pour les services autorisés par le gouvernement (forces civiles de sécurité, défense, infrastructures critiques etc.).

En outre, le projet de loi permettra un développement de l'industrie française en matière de radionavigation par satellite et de ses applications et augmentera les besoins en main-d'œuvre qualifiée dans ce secteur. Les entreprises du secteur pourront profiter du marché de l'ensemble des pays ayant mis en place un cadre normatif en la matière : la plupart des pays européens devraient s'en doter, et de grands pays hors de l'Union ont déjà manifesté leur intérêt (en particulier les Etats-Unis). Il convient de signaler, par exemple, que le développement de récepteurs bi-mode GPS et SPR est envisagé.

4.4 Impact administratif

Le SGDSN sera chargé de la mise en œuvre du dispositif et, à ce titre, délivrera les autorisations d'utilisation, de fabrication et de développement et d'exportation, et recevra les déclarations pour les transferts intracommunautaires.

Une cellule a d'ores et déjà été mise en place au sein de la direction des affaires internationales, stratégiques et technologiques, qui assure la liaison avec les instances européennes (dont l'agence européenne du GNSS[45] située à Prague) ainsi qu'avec les grands industriels français dans les secteurs de la technologie et de la défense.

Alors que d'autres pays s'orientent vers la création d'agences dédiées (Espagne), le choix d'une structure légère s'appuyant autant que possible sur des moyens existants a été fait, pour la France. Compte tenu de son rôle interministériel en matière de sécurité des programmes spatiaux, le SGDSN est apparu comme le meilleur positionnement pour assurer ces fonctions. Il s'appuiera en tant que de besoin sur l'expertise des autres ministères (notamment, le ministère des armées, qui dispose déjà d'une expérience de gestion de clefs sécurisées pour le GPS).

5. CONSULTATIONS MENEES

Aucune consultation obligatoire, hormis le Conseil d'Etat, n'est nécessaire pour ce projet de loi.

La consultation facultative de la commission supérieure de codification, qui peut être consultée sur les projets de textes modifiant des codes existants[46], n'a pas paru nécessaire en l'espèce, en l'absence de difficulté pour l'insertion de ces nouvelles dispositions dans le code de la défense.

[45] *Global Navigation Satellite System.*

[46] Article 1er du décret n°89-647 du 12 septembre 1989 relatif à la composition et au fonctionnement de la Commission supérieure de codification.

6. MODALITES DE MISE EN ŒUVRE

6.1 Textes d'application

Des dispositions réglementaires d'application seront nécessaires. Le projet de loi renvoie à un décret en Conseil d'Etat les conditions d'application des dispositions relatives aux activités contrôlées. Le décret désignera le SGDSN pour assurer cette mission, et précisera les modalités de procédure concernant les autorisations et déclarations prévues par la loi.

D'autres dispositions de la décision relèvent simplement de mesures d'application, comme la désignation d'autorités compétentes et la participation aux instances européennes de coopération créées par la directive.

6.2 Application dans le temps

La loi entrera en vigueur le lendemain de sa publication. Toutefois, ses dispositions ne seront pas directement applicables sans texte d'application.

6.3 Application dans l'espace

Les dispositions du projet de loi seraient applicables de plein droit dans les collectivités de l'article 73 de la Constitution (Guadeloupe, Guyane, Martinique, La Réunion, Mayotte) ainsi que dans les collectivités de l'article 74 de la Constitution qui sont régies par le principe de l'identité législative dans ce domaine (Saint-Barthélemy, Saint-Martin et Saint-Pierre-et-Miquelon).

En ce qui concerne les collectivités régies par le principe de spécialité législative (la Nouvelle-Calédonie, la Polynésie française, Wallis-et-Futuna et les Terres australes et antarctiques françaises), l'Etat est compétent en matière de sécurité publique. En conséquence, le présent projet de loi peut y être rendu applicable.

En ce qui concerne les dispositions du titre III relatif au service public réglementé de GALILEO, il convient de ne pas étendre les articles L. 2323-2 et L. 2323-5 créés par le présent projet aux collectivités relevant de la spécialité législative, en ce qu'ils sont relatifs au transfert intracommunautaire, transfert qui ne concerne pas les pays et territoires d'outre-mer.

La référence au règlement n° 428/2009 du Conseil du 5 mai 2009 dans le projet de loi doit faire l'objet de grilles de lectures. C'est l'objet des 2° à 5° du III de l'article 21.

Le contreseing de la ministre des outre-mer sera requis, dès lors que ce projet contient une mention d'application concernant les collectivités régies par le principe de spécialité législative.

ANNEXE I : TABLEAU SYNTHÉTIQUE DE PRÉSENTATION DES RÉGIMES ACTUELS D'ACQUISITION ET DE DÉTENTION DES DIFFÉRENTES CATÉGORIES D'ARMES

Armes de catégorie …		Régime actuel	Conditions pour être acquéreur et/ou détenteur	Exemples des principales armes figurant dans cette catégorie	Impact de la directive de 2017	
					Sur les conditions d'acquisition/détention	Sur les classements des armes dans les différentes catégories
A	A1	Interdiction	Certaines administrations ou services publics	Armes à feu de poing permettant le tir de plus de 21 munitions sans qu'intervienne un réapprovisionnement ; armes à feu d'épaule permettant le tir de plus de 31 munitions sans qu'intervienne un réapprovisionnement ;	Aucun	De nouvelles armes qui étaient classées en catégorie B vont relever de la catégorie A1.
	A2	Interdiction	Les experts judiciaires, les collectionneurs.	armes à feu de poing ou d'épaule à répétition automatique.	Aucun	Aucun
B		Autorisation	Tireurs sportifs, les personnes exposées à des risques exceptionnels d'atteinte à leur vie, les personnalités étrangères	B1° Armes à feu de poing ; B2° Armes à feu d'épaule à répétition semi-automatique d'une capacité supérieure à 3 coups ou équipées d'un système d'alimentation amovible et n'excédant pas 31 coups sans qu'intervienne un réapprovisionnement.	Aucun	Certaines armes qui relevaient de la catégorie B vont relever de la catégorie A1. Potentiellement, certaines répliques d'armes anciennes sont susceptibles

			séjournant en France ainsi que les personnes assurant leur sécurité, activités privées de sécurités, experts judiciaires, essais industriels, spectacle, fonctionnaires et agents publics .			d'entrer dans cette catégorie si elles remplissent certains critères fixés par la directive.
C		Déclaration	Permis de chasse et validation annuelle ou licence de tir sauf pour la catégorie C (3°).	Armes à feu d'épaule à répétition semi-automatique équipées de systèmes d'alimentation inamovibles permettant le tir de 3 munitions au plus ; armes à feu d'épaule à répétition manuelle équipées de systèmes d'alimentation permettant le tir de 11 munitions au plus.	Aucun	De nouvelles armes vont relever de cette catégorie (armes neutralisées, les répliques d'armes anciennes et les armes qui relevaient de la catégorie D (1°), principalement les armes de chasse.
D	D 1°	Enregistrement	Permis de chasse et validation annuelle ou licence de tir.	Armes d'épaule à canon lisse tirant un coup par canon	Aucun	Suppression de cette catégorie et surclassement en catégorie C

	D 2°	Liberté totale	Aucune	Tout objet susceptible de constituer une arme dangereuse (arme non à feu camouflées, poignards, matraques, projecteurs hypodermiques); générateurs d'aérosols incapacitants ou lacrymogènes < 100ml classés dans cette catégorie par arrêté ; armes à impulsion électrique classées par arrêté dans cette catégorie ; armes à feu neutralisées ; armes historiques et leurs reproductions ; armes et lanceurs non pyrotechniques (entre 2 et 20 joules) ; armes à blanc, à gaz, ou de signalisation, non convertible pour le tir de projectiles		Certaines armes relevant de la catégorie D2° font l'objet d'un surclassement en catégorie C (armes neutralisées). Les répliques d'armes historiques peuvent relever de toutes les catégories (A, B, C ou D)

ANNEXE II : TABLEAU DE TRANSPOSITION DE LA DIRECTIVE (UE) 2016/1148 DU PARLEMENT EUROPÉEN ET DU CONSEIL DU 6 JUILLET 2016 CONCERNANT DES MESURES DESTINEES A ASSURER UN NIVEAU ELEVE COMMUN DE SECURITE DES RESEAUX ET DES SYSTEMES D'INFORMATION DANS L'UNION

DISPOSITIONS DE LA DIRECTIVE	MESURE DE TRANSPOSITION PREVUE	OBSERVATIONS
CHAPITRE I **DISPOSITIONS GENERALES**		
Art. 1er, 1. La présente directive établit des mesures visant à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union afin d'améliorer le fonctionnement du marché intérieur.		
Art. 1er, 2. À cette fin, la présente directive: a) fixe des obligations à tous les États membres en ce qui concerne l'adoption d'une stratégie nationale en matière de sécurité des réseaux et des systèmes d'information; b) institue un groupe de coopération afin de soutenir et faciliter la coopération stratégique et l'échange d'informations entre les États membres et de renforcer la confiance mutuelle; c) institue un réseau des centres de réponse aux incidents de sécurité informatiques (ci-après dénommé «réseau des CSIRT») afin de contribuer au renforcement de la confiance entre les États membres et de promouvoir une coopération rapide et effective au niveau opérationnel; d) établit des exigences en matière de sécurité et de notification pour les opérateurs de services essentiels et pour les fournisseurs de service numérique; e) fixe des obligations aux États membres pour la désignation d'autorités nationales compétentes, de points de contact uniques et de CSIRT chargés de tâches liées à la sécurité des réseaux et des systèmes d'information.		

Art. 1er, 3. Les exigences en matière de sécurité et de notification prévues par la présente directive ne s'appliquent pas aux entreprises soumises aux exigences énoncées aux articles 13 bis et 13 ter de la directive 2002/21/CE ni aux prestataires de services de confiance soumis aux exigences énoncées à l'article 19 du règlement (UE) no 910/2014.	**Art. 2.** « Les dispositions du présent titre ne sont pas applicables aux entreprises exploitant des réseaux de communications électroniques publics ou fournissant des services de communications électroniques accessibles au public ni aux prestataires de services de confiance soumis aux exigences énoncées à l'article 19 du règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE.	Les fournisseurs de service numérique ne seront pas désignés par l'Etat ni ne se déclareront auprès de l'Etat. En conséquence, cette disposition vise à permettre à ces personnes de déterminer si elles sont dans le champ d'application de la présente directive. Les fournisseurs dont les services numériques sont déjà soumis à des exigences équivalentes de sécurité et de notification, en tant qu'opérateurs « télécom » ou prestataires « eIDAS », ne sont pas tenus d'appliquer les exigences correspondantes de la présente directive. Les opérateurs de services essentiels seront eux désignés par le Premier ministre qui tiendra compte de ces exceptions.
Art. 1er, 4. La présente directive est sans préjudice de la directive 2008/114/CE du Conseil et des directives du Parlement européen et du Conseil 2011/93/UE (15) et 2013/40/UE .		
Art. 1er, 5. Sans préjudice de l'article 346 du traité sur le fonctionnement de l'Union européenne, les informations considérées comme confidentielles en application de la réglementation nationale ou de l'Union, telle que les règles applicables au secret des affaires, ne peuvent faire l'objet d'un échange avec la Commission et d'autres autorités concernées que si cet échange est nécessaire à l'application de la présente directive. Les informations échangées se limitent au minimum nécessaire et sont proportionnées à l'objectif de cet échange. Cet échange d'informations préserve la confidentialité des informations concernées et protège la sécurité et les intérêts commerciaux des opérateurs de services essentiels et des fournisseurs de service	**Art. 3, al.2.** « Lorsqu'il informe le public ou les Etats membres de l'Union européenne d'incidents dans les conditions prévues aux articles 7 et 13, l'Etat tient compte des intérêts économiques de ces opérateurs et fournisseurs de service numérique et veille à ne pas révéler d'informations susceptibles de porter atteinte à leur sécurité et au secret en	

numérique.	matière commerciale et industrielle. » **Art. 3.** Les prestataires de service habilités à effectuer des contrôles dans le cadre de l'application du présent titre sont soumis aux mêmes règles de confidentialité que les services de l'Etat à l'égard des informations qu'ils recueillent auprès des opérateurs mentionnés à l'article 5 et des fournisseurs de service numérique mentionnés à l'article 11.	
Art. 1er, 6. La présente directive est sans préjudice des mesures prises par les États membres pour préserver leurs fonctions étatiques essentielles, en particulier dans le but de préserver la sécurité nationale, notamment les mesures visant à protéger les informations dont la divulgation est considérée par les États membres comme contraire aux intérêts essentiels de leur sécurité, et de maintenir l'ordre public, en particulier pour permettre la détection des infractions pénales ainsi que les enquêtes et les poursuites en la matière.		
Art. 1er, 7. Lorsqu'un acte juridique sectoriel de l'Union exige des opérateurs de services essentiels ou des fournisseurs de service numérique qu'ils assurent la sécurité de leurs réseaux et systèmes d'information ou qu'ils procèdent à la notification des incidents, à condition que les exigences en question aient un effet au moins équivalent à celui des obligations prévues par la présente directive, les dispositions de cet acte juridique sectoriel de l'Union s'appliquent.	**Art.2, al.2.** [Les dispositions du présent titre] ne sont pas non plus applicables aux réseaux et systèmes d'information des opérateurs de services essentiels et des fournisseurs de service numérique lorsque ces réseaux et systèmes d'information sont soumis à des exigences sectorielles de sécurité ou de notification des incidents ayant un effet au moins équivalent aux obligations résultant de l'application des dispositions du présent titre.	
Art. 2. 1. Le traitement de données à caractère personnel au titre de la présente directive est		

effectué conformément à la directive 95/46/CE. 2. Le traitement de données à caractère personnel par les institutions et organes de l'Union au titre de la présente directive est effectué conformément au règlement (CE) no 45/2001.		
Art. 3. Harmonisation minimale Sans préjudice de l'article 16, paragraphe 10, et des obligations qui leur incombent en vertu du droit de l'Union, les États membres peuvent adopter ou maintenir des dispositions en vue de parvenir à un niveau de sécurité plus élevé des réseaux et des systèmes d'information.	**Art. 5, al.2.** Les dispositions [du chapitre II] ne seront pas applicables aux systèmes d'information d'importance vitale mentionnés au premier alinéa de l'article L. 1332-6-1 du code de la défense.	
Art. 4. définitions Aux fins de la présente directive, on entend par: 1) «réseau et système d'information»: a) un réseau de communications électroniques au sens de l'article 2, point a), de la directive 2002/21/CE ; b) tout dispositif ou tout ensemble de dispositifs interconnectés ou apparentés, dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement automatisé de données numériques; ou c) les données numériques stockées, traitées, récupérées ou transmises par les éléments visés aux points a) et b) en vue de leur fonctionnement, utilisation, protection et maintenance; 2) «sécurité des réseaux et des systèmes d'information»: la capacité des réseaux et des systèmes d'information de résister, à un niveau de confiance donné, à des actions qui compromettent la disponibilité, l'authenticité, l'intégrité ou la confidentialité de données stockées, transmises ou faisant l'objet d'un traitement, et des services connexes que ces réseaux et systèmes d'information offrent ou rendent accessibles; 3) «stratégie nationale en matière de sécurité des réseaux et des systèmes d'information»: un cadre prévoyant des objectifs et priorités stratégiques en matière de sécurité des réseaux et des systèmes d'information au niveau national; 4) «opérateur de services essentiels»: une entité publique ou privée dont le type	**Art. 1er.** Pour l'application du présent titre, on entend par réseau et système d'information : 1° Tout réseau de communication électronique tel que défini au 2° de l'article L. 32 du code des postes et des communications électroniques ; 2° Tout dispositif ou tout ensemble de dispositifs interconnectés ou apparentés, dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement automatisé de données numériques ; 3° Les données numériques stockées, traitées, récupérées ou transmises par les éléments mentionnés aux 1° et 2° en vue de leur fonctionnement, utilisation, protection et maintenance. La sécurité des réseaux et systèmes d'information consiste en leur capacité	

figure à l'annexe II et qui répond aux critères énoncés à l'article 5, paragraphe 2; 5) «service numérique»: un service au sens de l'article 1er, paragraphe 1, point b), de la directive (UE) 2015/1535 du Parlement européen et du Conseil (17) dont le type figure dans la liste de l'annexe III; 6) «fournisseur de service numérique»: une personne morale qui fournit un service numérique; 7) «incident»: tout événement ayant un impact négatif réel sur la sécurité des réseaux et des systèmes d'information; 8) «gestion d'incident»: toutes les procédures utiles à la détection, à l'analyse et au confinement d'un incident et toutes les procédures utiles à l'intervention en cas d'incident; 9) «risque»: toute circonstance ou tout événement raisonnablement identifiable ayant un impact négatif potentiel sur la sécurité des réseaux et des systèmes d'information; 10) «représentant»: une personne physique ou morale établie dans l'Union qui est expressément désignée pour agir pour le compte d'un fournisseur de service numérique non établi dans l'Union, qui peut être contactée par une autorité nationale compétente ou un CSIRT à la place du fournisseur de service numérique concernant les obligations incombant audit fournisseur de service numérique en vertu de la présente directive; 11) «norme»: une norme au sens de l'article 2, point 1), du règlement (UE) no 1025/2012; 12) «spécification»: une spécification technique au sens de l'article 2, point 4), du règlement (UE) no 1025/2012; 13) «point d'échange internet» (IXP): une structure de réseau qui permet l'interconnexion de plus de deux systèmes autonomes indépendants, essentiellement aux fins de faciliter l'échange de trafic internet; un IXP n'assure l'interconnexion que pour des systèmes autonomes; un IXP n'exige pas que le trafic internet passant entre une paire quelconque de systèmes autonomes participants transite par un système autonome tiers, pas plus qu'il ne modifie ou n'altère par ailleurs un tel trafic; 14) «système de noms de domaine» (DNS): un système hiérarchique et distribué d'affectation de noms dans un réseau qui résout les questions liées aux noms de domaines; 15) «fournisseur de services DNS»: une entité qui fournit des services DNS sur l'internet; 16) «registre de noms de domaine de haut niveau»: une entité qui administre et gère l'enregistrement de noms de domaine internet dans un domaine de haut niveau donné;	de résister, à un niveau de confiance donné, à des actions qui compromettent la disponibilité, l'authenticité, l'intégrité ou la confidentialité de données stockées, transmises ou faisant l'objet d'un traitement, et des services connexes que ces réseaux et systèmes d'information offrent ou rendent accessibles. **Art. 10.** Pour l'application du présent chapitre, on entend : 1° Par service numérique tout service fourni normalement contre rémunération, à distance, par voie électronique et à la demande individuelle d'un destinataire de services ; 2° Par fournisseur de service numérique toute personne morale qui fournit l'un des services suivants : a) Place de marché en ligne à savoir un service numérique qui permet à des consommateurs ou à des professionnels au sens du a de l'article L. 151-1 du code de la consommation de conclure des contrats de vente ou de service en ligne avec des professionnels soit sur le site internet de la place de marché en ligne, soit sur le site internet d'un professionnel qui utilise les services informatiques fournis par la place de marché en ligne ; b) Moteurs de recherche en ligne à savoir un service numérique qui permet aux utilisateurs d'effectuer des recherches	

17) «place de marché en ligne»: un service numérique qui permet à des consommateurs et/ou à des professionnels au sens de l'article 4, paragraphe 1, point a) ou point b) respectivement, de la directive 2013/11/UE du Parlement européen et du Conseil (18) de conclure des contrats de vente ou de service en ligne avec des professionnels soit sur le site internet de la place de marché en ligne, soit sur le site internet d'un professionnel qui utilise les services informatiques fournis par la place de marché en ligne; 18) «moteur de recherche en ligne»: un service numérique qui permet aux utilisateurs d'effectuer des recherches sur, en principe, tous les sites internet ou sur les sites internet dans une langue donnée, sur la base d'une requête lancée sur n'importe quel sujet sous la forme d'un mot clé, d'une phrase ou d'une autre entrée, et qui renvoie des liens à partir desquels il est possible de trouver des informations en rapport avec le contenu demandé; 19) «service d'informatique en nuage»: un service numérique qui permet l'accès à un ensemble modulable et variable de ressources informatiques pouvant être partagées.	sur, en principe, tous les sites internet ou sur les sites internet dans une langue donnée, sur la base d'une requête lancée sur n'importe quel sujet sous la forme d'un mot clé, d'une phrase ou d'une autre entrée, et qui renvoie des liens à partir desquels il est possible de trouver des informations en rapport avec le contenu demandé ; c) Service d'informatique en nuage à savoir un service numérique qui permet l'accès à un ensemble modulable et variable de ressources informatiques pouvant être partagées.	
Art. 5, 1. Au plus tard le 9 novembre 2018, pour chaque secteur et sous-secteur visé à l'annexe II, les États membres identifient les opérateurs de services essentiels ayant un établissement sur leur territoire.	**Art. 24.** « Les **dispositions** des chapitres Ier et III du titre Ier entrent en vigueur à compter d'une date définie par décret en Conseil d'Etat et au plus tard le 9 mai 2018. La désignation des opérateurs de services essentiels prévue au 1er alinéa de l'article 5 intervient au plus tard le 9 novembre 2018. »	
Art. 5, 2. Les critères d'identification des opérateurs de services essentiels visés à l'article 4, point 4), sont les suivants: a) une entité fournit un service qui est essentiel au maintien d'activités sociétales et/ou économiques critiques; b) la fourniture de ce service est tributaire des réseaux et des systèmes d'information; et c) un incident aurait un effet disruptif important sur la fourniture dudit service.	**Art. 5.** Les opérateurs, publics ou privés, offrant des services essentiels au fonctionnement de la société ou de l'économie et qui pourraient être gravement perturbés par des incidents affectant les réseaux et systèmes d'information nécessaires à la fourniture de ces services sont soumis aux dispositions du présent chapitre pour	Les dispositions seront applicables aux systèmes d'information nécessaires à la fourniture des services essentiels qu'il s'agisse de systèmes exploités par les opérateurs eux-mêmes ou par leurs sous-traitants (conformément au considérant 52 de la directive). Le décret en CE : - fixera la liste des services essentiels.

	la sécurité de ces réseaux et systèmes d'information. Ces opérateurs sont désignés par le Premier ministre au regard des services qu'ils fournissent et des conséquences qu'auraient de tels incidents sur leurs services.	Elle sera élaborée à partir de l'annexe II de la directive ; - précisera les critères permettant de déterminer l'importance de la perturbation d'un service essentiel en cas d'incident (transposition de l'art. 6 de la directive) ; définira les conditions dans lesquelles seront désignés les opérateurs de services essentiels, et notamment les conditions dans lesquelles seront consultés les ministères pour la désignation de ces opérateurs.
Art. 5, 3. Aux fins du paragraphe 1, chaque État membre établit une liste des services visés au paragraphe 2, point a).	**Art. 5.** Les modalités d'application du présent titre sont déterminées par décret en Conseil d'Etat. Ce décret fixe notamment la liste des services essentiels au fonctionnement de la société ou de l'économie.	
Art 5, 4. Aux fins du paragraphe 1, lorsqu'une entité fournit un service visé au paragraphe 2, point a), dans deux États membres ou plus, les États membres en question se consultent mutuellement. La consultation intervient avant que l'identification ne fasse l'objet d'une décision.		
Art. 5, 5. À intervalles réguliers et au moins tous les deux ans à compter du 9 mai 2018, les États membres procèdent au réexamen et, au besoin, à la mise à jour de la liste des opérateurs de services essentiels identifiés.	**Art. 5.** « […] La liste de ces opérateurs est actualisée à intervalles réguliers et au moins tous les deux ans. »	
Art. 5, 6.		Cette coopération sera effectuée sous la

Le rôle du groupe de coopération consiste, conformément aux tâches visées à l'article 11, à aider les États membres à suivre une approche cohérente dans le processus d'identification des opérateurs de services essentiels.		coordination de l'Enisa avec les CSIRT.
Art. 5, 7. Aux fins du réexamen visé à l'article 23 et au plus tard le 9 novembre 2018, puis tous les deux ans, les États membres communiquent à la Commission les informations qui lui sont nécessaires pour évaluer la mise en œuvre de la présente directive, en particulier la cohérence des approches adoptées par les États membres pour l'identification des opérateurs de services essentiels. Ces informations comprennent au moins: a) les mesures nationales permettant l'identification des opérateurs de services essentiels; b) la liste des services visée au paragraphe 3; c) le nombre d'opérateurs de services essentiels identifiés pour chaque secteur visé à l'annexe II et une indication de leur importance pour ce secteur; d) les seuils, pour autant qu'ils existent, permettant de déterminer le niveau de l'offre pertinent en fonction du nombre d'utilisateurs tributaires de ce service visé à l'article 6, paragraphe 1, point a), ou de l'importance de cet opérateur de services essentiels particulier visée à l'article 6, paragraphe 1, point f). Afin de contribuer à la transmission d'informations comparables, la Commission peut, en tenant le plus grand compte de l'avis de l'ENISA, adopter des lignes directrices techniques appropriées concernant les paramètres applicables aux informations visées dans le présent paragraphe.		L'article 5 du projet de loi prévoit la réactualisation au niveau national de la liste des opérateurs de services essentiels. A cette occasion, les autorités françaises s'assureront de communiquer à la Commission les informations nécessaires pour procéder à l'évaluation de la mise en œuvre de la directive.
Art. 6. (effet disruptif important d'un incident) 1. Lorsque les États membres déterminent l'importance d'un effet disruptif visée à l'article 5, paragraphe 2, point c), ils prennent en compte au moins les facteurs transsectoriels suivants : a) le nombre d'utilisateurs tributaires du service fourni par l'entité concernée; b) la dépendance des autres secteurs visés à l'annexe II à l'égard du service fourni par cette entité; c) les conséquences que des incidents pourraient avoir, en termes de degré et de durée, sur les fonctions économiques ou sociétales ou sur la sûreté publique;	**Art. 7, al.1.** « Les opérateurs mentionnés à l'article 5 déclarent, sans retard injustifié, à l'autorité nationale de sécurité des systèmes d'information mentionnée à l'article L. 2321-1 du code de la défense, les incidents affectant les réseaux et systèmes d'information nécessaires à la fourniture de services essentiels, lorsque ces incidents ont ou sont susceptibles	Le Décret en CE précisera les critères permettant de désigner les OSE (rédaction indicative) : Pour déterminer l'importance de la perturbation d'un service essentiel fourni par un opérateur en cas d'incident affectant ses systèmes d'information, le Premier ministre tient compte des critères suivants :

d) la part de marché de cette entité; e) la portée géographique eu égard à la zone susceptible d'être touchée par un incident; f) l'importance que revêt l'entité pour garantir un niveau de service suffisant, compte tenu de la disponibilité de solutions de rechange pour la fourniture de ce service. 2. Afin de déterminer si un incident est susceptible d'avoir un effet disruptif important, les Etats membres prennent aussi en compte, le cas échéant, des facteurs sectoriels.	d'avoir, compte tenu notamment du nombre d'utilisateurs et de la zone géographique touchés ainsi que de la durée de l'incident, un impact significatif sur la continuité de ces services.»	a) le nombre d'utilisateurs dépendant du service fourni par l'opérateur de services essentiels ; b) la dépendance des autres secteurs d'activités à l'égard du service fourni par l'opérateur ; c) les conséquences que des incidents pourraient avoir, en termes de degré et de durée, sur les fonctions économiques ou sociétales ou sur la sûreté publique ; d) la part de marché de l'opérateur ; e) la portée géographique eu égard à la zone susceptible d'être touchée par un incident ; f) l'importance que revêt l'opérateur pour garantir un niveau de service suffisant, compte tenu de la disponibilité de solutions de rechange pour la fourniture de ce service ; [facteurs sectoriels à définir suite aux consultations en cours]
CHAPITRE II **CADRES NATIONAUX SUR LA SECURITE DES RESEAUX ET DES SYSTEMES D'INFORMATION**		Tous les éléments liés aux questions d'organisation et de gouvernance du chapitre II seront notifiés à la Commission européenne via le SGAE.
Art. 7. Stratégie nationale 1. Chaque État membre adopte une stratégie nationale en matière de sécurité des réseaux et des systèmes d'information qui définit les objectifs stratégiques et les mesures politiques et réglementaires appropriées en vue de parvenir à un niveau		La France s'est dotée d'une stratégie nationale pour la sécurité du numérique dès 2010, révisée en 2015 dans une démarche participative et

élevé de sécurité des réseaux et des systèmes d'information et de le maintenir et de couvrir au moins les secteurs visés à l'annexe II et les services visés à l'annexe III. La stratégie nationale en matière de sécurité des réseaux et des systèmes d'information porte, en particulier, sur les points suivants: a)les objectifs et les priorités de la stratégie nationale en matière de sécurité des réseaux et des systèmes d'information; b)un cadre de gouvernance permettant d'atteindre les objectifs et les priorités de la stratégie nationale en matière de sécurité des réseaux et des systèmes d'information, prévoyant notamment les rôles et les responsabilités des organismes publics et des autres acteurs pertinents; c)l'inventaire des mesures en matière de préparation, d'intervention et de récupération, y compris la coopération entre les secteurs public et privé; d)un aperçu des programmes d'éducation, de sensibilisation et de formation en rapport avec la stratégie nationale en matière de sécurité des réseaux et des systèmes d'information; e)un aperçu des plans de recherche et de développement en rapport avec la stratégie nationale en matière de sécurité des réseaux et des systèmes d'information; f) un plan d'évaluation des risques permettant d'identifier les risques; g)une liste des différents acteurs concernés par la mise en œuvre de la stratégie nationale en matière de sécurité des réseaux et des systèmes d'information. 2. Les États membres peuvent demander à l'ENISA de leur prêter assistance dans l'élaboration de leur stratégie nationale en matière de sécurité des réseaux et des systèmes d'information. 3. Les États membres communiquent leur stratégie nationale en matière de sécurité des réseaux et des systèmes d'information à la Commission dans un délai de trois mois suivant son adoption. Dans ce cadre, les États membres peuvent exclure des éléments de la stratégie se rapportant à la sécurité nationale.		interministérielle transversale entre toutes les administrations, qui répond aux aspirations et objectifs de l'article 7 de la directive. Cinq axes stratégiques : - 1. Intérêts fondamentaux, défense et sécurité des systèmes d'information de l'état et des infrastructures critiques, crise informatique majeure - 2. Confiance numérique, vie privée, données personnelles, cybermalveillance - 3. Sensibilisation, formations initiales, formations continues - 4. Environnement des entreprises du numérique, politique industrielle, export, internationalisation - 5. Europe, souveraineté numérique, stabilité du cyberespace
Art. 8. Autorités nationales compétentes et point de contact unique 1. Chaque État membre désigne une ou plusieurs autorités nationales compétentes en matière de sécurité des réseaux et des systèmes d'information (ci-après		L'ANSSI assurera les fonctions d'autorité nationale compétente et de

dénommées «autorités compétentes»), couvrant au moins les secteurs visés à l'annexe II et les services visés à l'annexe III. Les États membres peuvent attribuer cette mission à une ou des autorités existantes. 2. Les autorités compétentes contrôlent l'application de la présente directive au niveau national. 3. Chaque État membre désigne un point de contact national unique en matière de sécurité des réseaux et des systèmes d'information (ci-après dénommé «point de contact unique»). Les États membres peuvent attribuer cette mission à une autorité existante. Lorsqu'un État membre désigne une seule autorité compétente, cette dernière fait aussi fonction de point de contact unique. 4. Le point de contact unique exerce une fonction de liaison pour assurer une coopération transfrontalière entre les autorités des États membres, ainsi qu'avec les autorités concernées des autres États membres, le groupe de coopération visé à l'article 11 et le réseau des CSIRT visé à l'article 12. 5. Les États membres veillent à ce que les autorités compétentes et les points de contact uniques disposent de ressources suffisantes pour pouvoir s'acquitter de leurs tâches de manière effective et efficace et atteindre ainsi les objectifs de la présente directive. Les États membres font en sorte que les représentants désignés pour siéger au sein du groupe de coopération puissent coopérer de manière effective, efficace et sûre. 6. En fonction des besoins et conformément au droit national, les autorités compétentes et le point de contact unique consultent les services répressifs nationaux compétents et les autorités nationales chargées de la protection des données et coopèrent avec eux. 7. Chaque État membre notifie sans tarder à la Commission la désignation de l'autorité compétente et du point de contact unique, les tâches qui leur sont confiées et toute modification ultérieure dans ce cadre. Chaque État membre rend publique la désignation de l'autorité compétente et du point de contact unique. La Commission publie la liste des points de contact uniques désignés.		point de contact unique prévues à l'article 8 de la directive. Le décret n°2009-834 sur les missions de l'ANSSI sera être amendé pour étendre son champ d'action
Art. 9. CSIRT 1. Chaque État membre désigne un ou plusieurs CSIRT, se conformant aux exigences énumérées à l'annexe I, point 1), couvrant au moins les secteurs visés à l'annexe II et les services visés à l'annexe III, chargés de la gestion des incidents et des risques selon un processus bien défini. Un CSIRT peut être établi au sein d'une autorité compétente. 2. Les États membres veillent à ce que les CSIRT disposent de ressources		Le CERT-FR (ANSSI) est désigné comme CSIRT français répondant aux exigences prévues dans l'article 9 de la directive Il conviendra de compléter le décret

suffisantes pour pouvoir s'acquitter efficacement de leurs tâches énumérées à l'annexe I, point 2). Les États membres veillent à ce que leurs CSIRT coopèrent de manière effective, efficace et sécurisée au sein du réseau des CSIRT visé à l'article 12. 3. Les États membres font en sorte que leurs CSIRT aient accès à une infrastructure d'information et de communication adaptée, sécurisée et résiliente au niveau national. 4. Les États membres informent la Commission des missions de leurs CSIRT ainsi que des principaux éléments de leurs processus de gestion des incidents. 5. Les États membres peuvent solliciter l'assistance de l'ENISA pour la mise en place des CSIRT nationaux.		n°2009-834 relatif à l'ANSSI pour décrire le rôle du CSIRT.
Art. 10. 1. Lorsqu'ils sont distincts, l'autorité compétente, le point de contact unique et le CSIRT d'un même État membre coopèrent aux fins du respect des obligations énoncées dans la présente directive. 2. Les États membres veillent à ce que soit les autorités compétentes, soit les CSIRT reçoivent les notifications d'incidents transmises en application de la présente directive. Lorsqu'un État membre décide que les CSIRT ne reçoivent pas de notifications, ils se voient accorder, dans la mesure nécessaire à l'accomplissement de leurs tâches, un accès aux données relatives aux incidents notifiés par les opérateurs de services essentiels au titre de l'article 14, paragraphes 3 et 5, ou par les fournisseurs de service numérique au titre de l'article 16, paragraphes 3 et 6. 3. Les États membres veillent à ce que les autorités compétentes ou les CSIRT informent les points de contact uniques des notifications d'incidents transmises en application de la présente directive. Au plus tard le 9 août 2018, puis tous les ans, le point de contact unique transmet au groupe de coopération un rapport de synthèse sur les notifications reçues, y compris le nombre de notifications et la nature des incidents notifiés, ainsi que sur les mesures prises conformément à l'article 14, paragraphes 3 et 5, et à l'article 16, paragraphes 3 et 6.	**Art 7, al.2.** « En outre, lorsqu'un incident a un impact significatif sur la continuité de services essentiels fournis par l'opérateur à d'autres Etats membres de l'Union européenne, le Premier ministre en informe les autorités ou organismes compétents de ces Etats. »	
CHAPITRE III **COOPERATION**		
Art. 11. 1. Un groupe de coopération est institué aux fins de soutenir et de faciliter la coopération stratégique et l'échange d'informations entre les États membres et de renforcer la confiance, et de parvenir à un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union.		L'ANSSI représentera la France dans le groupe de coopération, cette dernière participe déjà pleinement à la coopération existante avec l'ENISA, son

Le groupe de coopération exécute ses tâches en s'appuyant sur les programmes de travail bisannuels visés au paragraphe 3, deuxième alinéa. 2. Le groupe de coopération est composé de représentants des États membres, de la Commission et de l'ENISA. Si besoin est, le groupe de coopération peut inviter des représentants des acteurs concernés à participer à ses travaux. Le secrétariat est assuré par la Commission. 3. Le groupe de coopération est chargé des tâches suivantes: a) fournir des orientations stratégiques pour les activités du réseau des CSIRT institué en vertu de l'article 12; b) échanger les bonnes pratiques concernant l'échange d'informations sur les notifications d'incidents visé à l'article 14, paragraphes 3 et 5, et à l'article 16, paragraphes 3 et 6; c) échanger les bonnes pratiques entre les États membres et, en coopération avec l'ENISA, aider les États membres à renforcer leurs capacités en matière de sécurité des réseaux et des systèmes d'information; d) discuter des capacités et de l'état de préparation des États membres et, à titre volontaire, évaluer les stratégies nationales en matière de sécurité des réseaux et des systèmes d'information et l'efficacité des CSIRT, et identifier les bonnes pratiques; e) échanger des informations et les bonnes pratiques en matière de sensibilisation et de formation; f) échanger des informations et les bonnes pratiques en matière de recherche et de développement dans le domaine de la sécurité des réseaux et des systèmes d'information; g) le cas échéant, procéder à des échanges d'expériences sur des questions relatives à la sécurité des réseaux et des systèmes d'information avec les institutions, organes ou organismes de l'Union concernés; h) discuter des normes et des spécifications visées à l'article 19 avec les représentants des organismes de normalisation européens concernés; i) recueillir des informations sur les bonnes pratiques en matière de risques et d'incidents; j) examiner chaque année les rapports de synthèse visés à l'article 10, paragraphe 3, deuxième alinéa; k) discuter du travail accompli en ce qui concerne les exercices relatifs à la sécurité		rôle sera donc naturellement étendue.

des réseaux et des systèmes d'information, les programmes d'éducation et la formation, y compris le travail réalisé par l'ENISA; l) avec l'assistance de l'ENISA, échanger les bonnes pratiques concernant l'identification, par les États membres, des opérateurs de services essentiels, y compris au regard des dépendances transfrontalières, en matière de risques et d'incidents; m) discuter des modalités de signalement des notifications d'incidents visées aux articles 14 et 16. Au plus tard le 9 février 2018, puis tous les deux ans, le groupe de coopération établit un programme de travail prévoyant les actions à entreprendre pour mettre en œuvre les objectifs et les tâches et qui est cohérent avec les objectifs de la présente directive. 4. Aux fins du réexamen visé à l'article 23 et au plus tard le 9 août 2018, puis tous les ans et demi, le groupe de coopération établit un rapport évaluant l'expérience acquise à la suite de la coopération stratégique visée au présent article. 5. La Commission adopte des actes d'exécution fixant les modalités de procédure nécessaires au fonctionnement du groupe de coopération. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 22, paragraphe 2. Aux fins du premier alinéa, la Commission présente au comité visé à l'article 22, paragraphe 1, le premier projet d'acte d'exécution le 9 février 2017 au plus tard.		
Art. 12. 1. Afin de contribuer au renforcement de la confiance entre les États membres et de promouvoir une coopération opérationnelle rapide et effective, un réseau des CSIRT nationaux est établi. 2. Le réseau des CSIRT est composé de représentants des CSIRT des États membres et du CERT-UE. La Commission participe au réseau des CSIRT en qualité d'observateur. L'ENISA assure le secrétariat et soutient activement la coopération entre les CSIRT .3. Le réseau des CSIRT est chargé des tâches suivantes: a) échanger des informations sur les services, les opérations et les capacités de coopération des CSIRT; b) à la demande du représentant d'un CSIRT d'un État membre susceptible d'être touché par un incident, échanger des informations non sensibles d'un point de vue commercial en rapport avec l'incident en question et les risques correspondants et en débattre; toutefois, un CSIRT d'un État membre peut refuser de contribuer à ce débat s'il existe un risque de porter atteinte à l'enquête sur l'incident;		Le CERT-FR (ANSSI) représentera la France au sein du réseau des CSIRTs des Etats membres de l'Union européenne. Cette représentation sera notifiée à la Commission et, au niveau national, le décret n°2009-834 sera modifié pour tenir compte de ce rôle.

c) échanger et mettre à disposition, à titre volontaire, des informations non confidentielles sur les différents incidents; d) à la demande du représentant d'un CSIRT d'un État membre, discuter et, si possible, identifier une réponse coordonnée à un incident identifié qui relève de la juridiction de ce même État membre; e) aider les États membres à faire face à des incidents transfrontaliers sur la base d'une assistance mutuelle volontaire; f) débattre, étudier et identifier d'autres formes de coopération opérationnelle, notamment en rapport avec: i) les catégories de risques et d'incidents; ii) les alertes précoces; iii) l'assistance mutuelle; iv) les principes et modalités d'une coordination lorsque les États membres réagissent à des risques et incidents transfrontaliers; g) informer le groupe de coopération des activités du réseau et des autres formes de coopération opérationnelle débattues en application du point f) et demander des orientations à cet égard; h) étudier les enseignements tirés des exercices relatifs à la sécurité des réseaux et des systèmes d'information, y compris de ceux organisés par l'ENISA; i) à la demande d'un CSIRT donné, étudier les capacités et l'état de préparation dudit CSIRT; j) publier des lignes directrices afin de faciliter la convergence des pratiques opérationnelles en ce qui concerne l'application des dispositions du présent article relatives à la coopération opérationnelle. 4. Aux fins du réexamen visé à l'article 23 et au plus tard le 9 août 2018, puis tous les ans et demi, le réseau des CSIRT établit un rapport évaluant l'expérience acquise à la suite de la coopération opérationnelle visée au présent article, comprenant des conclusions et des recommandations. Ce rapport est aussi transmis au groupe de coopération. 5. Le réseau des CSIRT établit son propre règlement intérieur.		
Art. 13. Coopération internationale L'Union peut, conformément à l'article 218 du traité sur le fonctionnement de l'Union européenne, conclure, avec des pays tiers ou des organisations internationales, des accords internationaux qui permettent et organisent leur participation à certaines activités du groupe de coopération. Ces accords tiennent compte de la nécessité		

d'assurer un niveau suffisant de protection des données.		
CHAPITRE IV SÉCURITÉ DES RÉSEAUX ET DES SYSTÈMES D'INFORMATION DES OPÉRATEURS DE SERVICES ESSENTIELS		
Art. 14, 1 et 2. (exigences de sécurité) 1. Les États membres veillent à ce que les opérateurs de services essentiels prennent les mesures techniques et organisationnelles nécessaires et proportionnées pour gérer les risques qui menacent la sécurité des réseaux et des systèmes d'information qu'ils utilisent dans le cadre de leurs activités. Ces mesures garantissent, pour les réseaux et les systèmes d'information, un niveau de sécurité adapté au risque existant, compte tenu de l'état des connaissances. 2. Les États membres veillent à ce que les opérateurs de services essentiels prennent les mesures appropriées en vue de prévenir les incidents qui compromettent la sécurité des réseaux et des systèmes d'information utilisés pour la fourniture de ces services essentiels ou d'en limiter l'impact, en vue d'assurer la continuité de ces services.	**Art. 6.** « Le Premier ministre fixe les règles de sécurité nécessaires à la protection des réseaux et systèmes d'information mentionnés au premier alinéa de l'article 5. Ces règles ont pour objet de garantir un niveau de sécurité adapté au risque existant, compte tenu de l'état des connaissances. Elles définissent les mesures appropriés pour prévenir les incidents qui compromettent la sécurité des réseaux et systèmes d'information utilisés pour la fourniture des services essentiels ou pour en limiter l'impact afin d'assurer la continuité de ces services essentiels. Les opérateurs mentionnés au même article appliquent ces règles à leurs frais. Les règles prévues au premier alinéa peuvent notamment prescrire que les opérateurs recourent à des dispositifs matériels ou logiciels ou à des services informatiques dont la sécurité a été certifiée. »	Les règles fixées par le Premier ministre imposeront notamment aux opérateurs de prendre les mesures techniques et organisationnelles nécessaires et proportionnées pour gérer les risques qui menacent la sécurité des réseaux et des systèmes d'information qu'ils utilisent dans le cadre de leurs activités (transposition de l'art. 14.1 de la directive). Ces règles imposeront également aux opérateurs de prendre les mesures appropriées en vue de prévenir les incidents qui compromettent la sécurité des réseaux et des systèmes d'information utilisés pour la fourniture de services essentiels ou d'en limiter l'impact, en vue d'assurer la continuité de ces services (transposition de l'art. 14.2 de la directive). Le décret en CE : - précisera que les règles seront fixées par arrêté du Premier ministre ; - précisera que ces règles s'appliqueront aux seuls systèmes d'information nécessaires pour fournir les services essentiels et pour lesquels un incident pourrait

		perturber gravement la fourniture des services. Ces systèmes seront appelés « systèmes d'information essentiels » ; - imposera aux opérateurs d'élaborer et de tenir à jour la liste de leurs systèmes d'information essentiels et de la communiquer à l'ANSSI sur demande ; - définira la procédure de certification des dispositifs matériels ou logiciels et des services informatiques auxquels recourent les opérateurs.
Art. 14, 3 et 4. (notification et évaluation d'impacts des incidents) 3) Les États membres veillent à ce que les opérateurs de services essentiels notifient à l'autorité compétente ou au CSIRT, sans retard injustifié, les incidents qui ont un impact significatif sur la continuité des services essentiels qu'ils fournissent. Les notifications contiennent des informations permettant à l'autorité compétente ou au CSIRT de déterminer si l'incident a un impact au niveau transfrontalier. 4) Afin de déterminer l'ampleur de l'impact d'un incident, il est, en particulier, tenu compte des paramètres suivants : a) le nombre d'utilisateurs touchés par la perturbation du service essentiel; b) la durée de l'incident; c) la portée géographique eu égard à la zone touchée par l'incident.	**Art 7, al.1.** Les opérateurs mentionnés à l'article 5 déclarent, sans retard injustifié, à l'autorité nationale de sécurité des systèmes d'information mentionnée à l'article L. 2321-1 du code de la défense, les incidents affectant les réseaux et systèmes d'information nécessaires à la fourniture de services essentiels, lorsque ces incidents ont ou sont susceptibles d'avoir, compte tenu notamment du nombre d'utilisateurs et de la zone géographique touchés ainsi que de la durée de l'incident, un impact significatif sur la continuité de ces services.	Le décret en CE : - fixera les modalités de déclaration des incidents et précisera les informations à communiquer, en particulier celles qui permettent de déterminer si l'incident a un impact au niveau transfrontalier ; - précisera les paramètres permettant de déterminer l'ampleur de l'impact d'un incident ; - précisera les conditions dans lesquelles seront communiquées aux ministères concernés les informations relatives aux incidents.
Art. 14, 5. (information des Etats membres en cas d'incidents ayant des impacts transfrontières) Sur la base des informations fournies dans la notification de l'opérateur de services essentiels, l'autorité compétente ou le CSIRT signale aux autres États membres	**Art. 3, al.2.** « Lorsqu'il informe le public ou les Etats membres de l'Union européenne d'incidents dans les conditions prévues	

touchés si l'incident a un impact significatif sur la continuité des services essentiels dans ces États membres. Ce faisant, l'autorité compétente ou le CSIRT doit, dans le respect du droit de l'Union ou de la législation nationale conforme au droit de l'Union, préserver la sécurité et les intérêts commerciaux de l'opérateur de services essentiels ainsi que la confidentialité des informations communiquées dans sa notification.	aux articles 7 et 13, l'Etat tient compte des intérêts économiques de ces opérateurs et fournisseurs de service numérique et veille à ne pas révéler d'informations susceptibles de porter atteinte à leur sécurité et au secret en matière commerciale et industrielle. » Art. 7, al.2« En outre, lorsqu'un incident a un impact significatif sur la continuité de services essentiels fournis par l'opérateur à d'autres Etats membres de l'Union européenne, le Premier ministre en informe les autorités ou organismes compétents de ces Etats. »	
Art. 14, 5. (traitement des incidents) Lorsque les circonstances le permettent, l'autorité compétente ou le CSIRT fournit à l'opérateur de services essentiels qui est à l'origine de la notification des informations utiles au suivi de sa notification, par exemple celles qui pourraient contribuer à une gestion efficace de l'incident.		Décret en CE (rédaction indicative) Lorsque les circonstances le permettent, l'ANSSI fournit à l'opérateur de services essentiels qui est à l'origine de la déclaration des informations utiles au suivi de sa déclaration, par exemple celles qui pourraient contribuer à une gestion efficace de l'incident.
Art. 14, 6. (information du public en cas d'incidents) Après avoir consulté l'opérateur de services essentiels qui est à l'origine de la notification, l'autorité compétente ou le CSIRT peut informer le public concernant des incidents particuliers, lorsque la sensibilisation du public est nécessaire pour prévenir un incident ou gérer un incident en cours.	**Art. 7.** Après avoir consulté l'opérateur concerné, le Premier ministre peut informer le public d'un incident mentionné au premier alinéa, lorsque cette information est nécessaire pour prévenir ou traiter un incident.	
Art. 15, 1 et 2. (mise en œuvre et exécution) : 1. Les États membres veillent à ce que les autorités compétentes disposent des pouvoirs et des moyens nécessaires pour évaluer le respect, par les opérateurs de	**Art. 8.** Le Premier ministre peut soumettre les opérateurs mentionnés à l'article 5 à des contrôles destinés à vérifier le respect	Le décret en CE : - définira les modalités des contrôles (notification, déroulement, rapport,

services essentiels, des obligations qui leur incombent en vertu de l'article 14, ainsi que les effets de ce respect sur la sécurité des réseaux et des systèmes d'information. 2. Les États membres veillent à ce que les autorités compétentes disposent des pouvoirs et des moyens leur permettant d'exiger des opérateurs de services essentiels qu'ils fournissent : a) les informations nécessaires pour évaluer la sécurité de leurs réseaux et systèmes d'information, y compris les documents relatifs à leurs politiques de sécurité; b) des éléments prouvant la mise en œuvre effective des politiques de sécurité, tels que les résultats d'un audit de sécurité exécuté par l'autorité compétente ou un auditeur qualifié et, dans ce dernier cas, qu'ils en mettent les résultats, y compris les éléments probants, à la disposition de l'autorité compétente. Au moment de formuler une telle demande d'informations et de preuves, l'autorité compétente mentionne la finalité de la demande et précise quelles sont les informations exigées.	des obligations prévues par le présent chapitre ainsi que le niveau de sécurité des réseaux et systèmes d'information nécessaires à la fourniture de services essentiels. Les contrôles sont effectués, sur pièce et sur place, par l'autorité nationale de sécurité des systèmes d'information mentionnée à l'article L. 2321-1 du code de la défense ou par des prestataires de service qualifiés. Le coût des contrôles est à la charge des opérateurs. La qualification de prestataire de service habilité à effectuer ces contrôles est délivrée par le Premier ministre. Les opérateurs sont tenus de communiquer à l'autorité ou au prestataire de service chargé du contrôle prévu au premier alinéa les informations et éléments nécessaires pour réaliser le contrôle, y compris les documents relatifs à leur politique de sécurité et les résultats d'audit de sécurité et leur permettre d'accéder aux réseaux et systèmes d'information soumis au contrôle afin d'effectuer des analyses et des relevés d'informations techniques.	etc.). Il précisera les informations à fournir par les opérateurs (politique de sécurité des systèmes d'information, documentation technique, etc.) et les modalités d'accès aux systèmes d'information contrôlés ; - précisera que les rapports des contrôles sont remis à l'ANSSI dans les cas où elle n'effectue pas elle-même le contrôle ; - définira la procédure de qualification par le Premier ministre des prestataires de service de contrôle ; - fixera le coût des contrôles effectués par l'ANSSI par arrêté du Premier ministre ; - précisera les conditions dans lesquelles seront communiquées aux ministères concernés les informations relatives aux résultats des contrôles.
Art. 15, 3. (instructions contraignantes) : Après évaluation des informations ou des résultats des audits de sécurité visés au paragraphe 2, l'autorité compétente peut donner des instructions contraignantes aux opérateurs de services essentiels pour remédier aux défaillances identifiées.	**Art. 8, al.4.** Les opérateurs corrigent tout manquement à leurs obligations qui aurait été ainsi constaté dans le délai imparti par la mise en demeure notifiée à l'issue du contrôle.	
CHAPITRE V SÉCURITÉ DES RÉSEAUX ET DES SYSTÈMES D'INFORMATION DES FOURNISSEURS DE SERVICE NUMÉRIQUE		
Art. 16, 1 et 2. (exigences de sécurité) :	**Art. 12.**	Les dispositions seront applicables aux

1. Les États membres veillent à ce que les fournisseurs de service numérique identifient les risques qui menacent la sécurité des réseaux et des systèmes d'information qu'ils utilisent pour offrir, dans l'Union, les services visés à l'annexe III, et prennent les mesures techniques et organisationnelles nécessaires et proportionnées pour les gérer. Ces mesures garantissent, compte tenu de l'état des connaissances, un niveau de sécurité des réseaux et des systèmes d'information adapté au risque existant et prennent en considération les éléments suivants : a) la sécurité des systèmes et des installations; b) la gestion des incidents; c) la gestion de la continuité des activités; d) le suivi, l'audit et le contrôle; e) le respect des normes internationales. 2. Les États membres veillent à ce que les fournisseurs de service numérique prennent des mesures pour éviter les incidents portant atteinte à la sécurité de leurs réseaux et systèmes d'information, et réduire au minimum l'impact de ces incidents sur les services visés à l'annexe III qui sont offerts dans l'Union, de manière à garantir la continuité de ces services.	Les fournisseurs de service numérique mentionnés à l'article 11 garantissent, compte tenu de l'état des connaissances, un niveau de sécurité des réseaux et des systèmes d'information nécessaires à la fourniture de leurs services dans l'Union européenne adapté aux risques existants. A cet effet, ils identifient les risques qui menacent la sécurité de ces réseaux et systèmes d'information et prennent les mesures techniques et organisationnelles nécessaires et proportionnées pour gérer ces risques. Ces mesures prennent notamment en considération la sécurité des systèmes et des installations, la gestion des incidents, la gestion de la continuité des activités, le suivi, l'audit et le contrôle ainsi que le respect des normes internationales. Les fournisseurs de service numérique prennent en outre les mesures utiles destinées, d'une part, à éviter les incidents de nature à porter atteinte à la sécurité des réseaux et systèmes d'information nécessaires à la fourniture de leurs services dans l'Union européenne et, d'autre part, à en réduire au minimum l'impact, de manière à garantir la continuité de ces services.	systèmes d'information nécessaires à la fourniture des services numériques qu'il s'agisse de systèmes exploités par les fournisseurs de service eux-mêmes ou par leurs sous-traitants (conformément au considérant 52 de la directive). Les éléments d'appréciation du niveau de sécurité nécessaire, en particulier l'énumération indicative de la directive, seront précisés dans le décret d'application.
Art. 16, 3 et 4. (notification d'incidents et évaluation des impacts) : 3) Les États membres veillent à ce que les fournisseurs de service numérique notifient à l'autorité compétente ou au CSIRT, sans retard injustifié, tout incident ayant un impact significatif sur la fourniture d'un service visé à l'annexe III qu'ils offrent dans l'Union. Les notifications contiennent des informations permettant à l'autorité compétente ou au CSIRT d'évaluer l'ampleur de l'éventuel impact au niveau	**Art. 13.** Les fournisseurs de service numérique mentionnés à l'article 11 déclarent, sans retard injustifié, à l'autorité nationale de sécurité des systèmes d'information mentionnée à l'article L. 2321-1 du code de la défense, les incidents affectant les	Le décret en CE : - fixera les modalités de déclaration des incidents et précisera les informations à communiquer, en particulier celles qui permettent d'évaluer l'ampleur de l'impact au

transfrontalier. 4) Afin de déterminer l'importance de l'impact d'un incident, il convient de tenir compte, en particulier, des paramètres qui suivent: a) le nombre d'utilisateurs touchés par l'incident, en particulier ceux qui recourent au service pour la fourniture de leurs propres services; b) la durée de l'incident; c) la portée géographique eu égard à la zone touchée par l'incident; d) la gravité de la perturbation du fonctionnement du service; e) l'ampleur de l'impact sur les fonctions économiques et sociétales. L'obligation de notifier un incident ne s'applique que lorsque le fournisseur de service numérique a accès aux informations nécessaires pour évaluer l'impact de l'incident eu égard aux paramètres visés au premier alinéa.	réseaux et systèmes d'information nécessaires à la fourniture de leurs services dans l'Union européenne, lorsque les informations dont ils disposent font apparaître que ces incidents ont un impact significatif sur la fourniture de ces services, compte tenu notamment du nombre d'utilisateurs touchés par l'incident, de sa durée, de sa portée géographique, de la gravité de la perturbation du fonctionnement du service et de son impact sur le fonctionnement de la société ou de l'économie.	niveau transfrontalier ; - précisera les paramètres permettant de déterminer l'importance de l'impact d'un incident (transposition de l'art. 16.4 de la directive) ; - précisera les conditions dans lesquelles seront communiquées aux ministères concernés les informations relatives aux incidents.
Art 16, 5. Lorsqu'un opérateur de services essentiels s'appuie sur un tiers fournisseur de service numérique pour la prestation d'un service essentiel au maintien de fonctions sociétales et économiques critiques, tout impact significatif sur la continuité des services essentiels en raison d'un incident touchant le fournisseur de service numérique est notifié par ledit opérateur.		L'article 3 du projet de loi prévoit que les opérateurs déclarent les incidents affectant les systèmes nécessaires à la fourniture de leurs services. Cette disposition s'applique que ces systèmes soient gérés par l'opérateur ou par un tiers. Ainsi que le précisera le décret d'application, l'opérateur aura la responsabilité de faire appliquer à ces tiers sous-traitants (par la voie contractuelle), les dispositions auxquelles il est soumis47. En particulier, un tiers qui exploite des systèmes pour le compte d'un opérateur devra l'informer des incidents affectant ces systèmes afin de permettre à cet opérateur de déclarer à l'ANSSI ces incidents.
Art. 16, 6. (information des Etats membres en cas d'incidents ayant des impacts	**Art. 13, al.2.**	

[47] Voir sur ce point considérant 52.

transfrontières) : Lorsque c'est approprié, et notamment si l'incident visé au paragraphe 3 concerne deux États membres ou plus, l'autorité compétente ou le CSIRT informe les autres États membres touchés. Ce faisant, les autorités compétentes, les CSIRT et les points de contact uniques doivent, dans le respect du droit de l'Union ou de la législation nationale conforme au droit de l'Union, préserver la sécurité et les intérêts commerciaux du fournisseur de service numérique ainsi que la confidentialité des informations communiquées.	Après avoir consulté le fournisseur de service numérique concerné, le Premier ministre peut informer le public d'un incident mentionné au premier alinéa ou imposer au fournisseur de le faire, lorsque cette information est nécessaire pour prévenir ou traiter un incident ou est justifiée par un motif d'intérêt général. En outre, lorsqu'un incident a des conséquences significatives sur les services fournis à d'autres Etats membres de l'Union européenne, le Premier ministre en informe les autorités ou organismes compétents de ces Etats, qui peuvent rendre public l'incident.	
Art. 16, 7. (information du public en cas d'incidents) Après avoir consulté le fournisseur de service numérique concerné, l'autorité compétente ou le CSIRT et, lorsque c'est approprié, les autorités ou les CSIRT des autres États membres concernés peuvent informer le public d'incidents particuliers ou imposer au fournisseur de service numérique de le faire, dans le cas où la sensibilisation du public est nécessaire pour prévenir un incident ou pour gérer un incident en cours, ou lorsque la divulgation de l'incident est dans l'intérêt public à d'autres égards.	**Art. 3, al.2.** Lorsqu'il informe le public ou les Etats membres de l'Union européenne d'incidents dans les conditions prévues aux articles 7 et 13, l'Etat tient compte des intérêts économiques de ces opérateurs et fournisseurs de service numérique et veille à ne pas révéler d'informations susceptibles de porter atteinte à leur sécurité et au secret en matière commerciale et industrielle.	
Art. 16, 8, 9 et 10. (actes d'exécution complétant l'art. 16,1 et 4) : La Commission adopte des actes d'exécution afin de compléter les éléments visés au paragraphe 1 et les paramètres énumérés au paragraphe 4 du présent article. 9. La Commission peut adopter des actes d'exécution fixant les formats et les procédures à appliquer pour respecter les exigences en matière de notification. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 22, paragraphe 2.		Des dispositions de nature règlementaire complèteront la transposition de l'art. 16.1 et de l'art. 16.4 de la directive. Elles ne pourront être prises qu'après la publication des actes d'exécution fixée au plus tard le 9 août 2017.

10. Sans préjudice de l'article 1er, paragraphe 6, les États membres n'imposent pas aux fournisseurs de service numérique d'autres exigences liées à la sécurité ou aux notifications.		
Art. 16, 11. (exception pour les micro et petites entreprises) : Le chapitre V ne s'applique pas aux microentreprises et petites entreprises telles qu'elles sont définies dans la recommandation 2003/361/CE de la Commission.	**Art. 11, al.2.** « Les dispositions du présent chapitre ne sont pas applicables aux entreprises qui emploient moins de 50 salariés et dont le chiffre d'affaires annuel n'excède pas 10 millions d'euros. »	Les fournisseurs de service numérique ne seront pas désignés par l'Etat ni ne se déclareront auprès de l'Etat. En conséquence, cette disposition vise à permettre à ces personnes de déterminer si elles sont dans le champ d'application de la présente directive. Pour la définition des micro et petites entreprises, il est proposé de renvoyer directement à la disposition concernée de la directive en l'absence de définitions équivalentes dans la réglementation nationale, notamment s'agissant des petites entreprises.
Art. 17, 1 et 2. (mise en œuvre et exécution) : 1. Les États membres veillent à ce que les autorités compétentes prennent des mesures, au besoin, dans le cadre de mesures de contrôle a posteriori, lorsque, selon les éléments communiqués, un fournisseur de service numérique ne satisfait pas aux exigences énoncées à l'article 16. Ces éléments peuvent être communiqués par une autorité compétente d'un autre État membre dans lequel le service est fourni. 2. Aux fins du paragraphe 1, les autorités compétentes disposent des pouvoirs et des moyens nécessaires pour imposer aux fournisseurs de service numérique : a) de communiquer les informations nécessaires pour évaluer la sécurité de leurs réseaux et systèmes d'information, y compris les documents relatifs à leurs politiques de sécurité ; b) de corriger tout manquement aux obligations fixées à l'article 16.	**Art. 14.** Lorsque le Premier ministre est informé qu'un fournisseur de service numérique mentionné à l'article 11 ne satisfait pas à l'une des obligations prévues aux articles 12 ou 13, il peut le soumettre à des contrôles destinés à vérifier le respect des obligations prévues par le présent chapitre ainsi que le niveau de sécurité des réseaux et systèmes d'information nécessaires à la fourniture de ces services. Il en informe si nécessaire les autorités compétentes des autres Etats membres dans lesquels sont situés des réseaux et systèmes d'information de ce	Le décret en CE : - définira les modalités des contrôles (notification, déroulement, rapport, etc.). Il précisera les informations à fournir par les fournisseurs de service numérique (politique de sécurité des systèmes d'information, documentation technique, etc.) et les modalités d'accès aux systèmes d'information contrôlés ; - précisera que les rapports des contrôles sont remis à l'ANSSI dans les cas où elle n'effectue pas elle-même le contrôle ; - définira la procédure de qualification

	fournisseur et coopère avec elles. Les contrôles sont effectués, sur pièce et sur place, par l'autorité nationale de sécurité des systèmes d'information mentionnée à l'article L. 2321-1 du code de la défense ou par des prestataires de service qualifiés. Le coût des contrôles est à la charge des fournisseurs de service numérique. La qualification de prestataire de service habilité à effectuer ces contrôles est délivrée par le Premier ministre. Les fournisseurs de service numérique sont tenus de communiquer à l'autorité ou au prestataire de service chargé du contrôle prévu au premier alinéa, les informations nécessaires pour évaluer la sécurité de leurs réseaux et systèmes d'information, y compris les documents relatifs à leurs politiques de sécurité de leur permettre d'accéder aux réseaux et systèmes d'information soumis au contrôle afin d'effectuer des analyses et des relevés d'informations techniques. Ils corrigent tout manquement à leurs obligations qui aurait été ainsi constaté dans le délai imparti par la mise en demeure notifiée à l'issue du contrôle.	par le Premier ministre des prestataires de service de contrôle ; - fixera le coût des contrôles effectués par l'ANSSI par arrêté du Premier ministre ; - précisera les conditions dans lesquelles seront communiquées aux ministères concernés les informations relatives aux résultats des contrôles.
Art. 18, 1 et 2. (compétence et territorialité) : 1. Aux fins de la présente directive, un fournisseur de service numérique est considéré comme relevant de la compétence de l'État membre dans lequel il a son établissement principal. Un fournisseur de service numérique est réputé	**Art. 11.** Sont soumis aux dispositions du présent chapitre les fournisseurs de service numérique offrant leurs services dans	Les fournisseurs de service numérique ne seront pas désignés par l'Etat ni ne se déclareront auprès de l'Etat. En conséquence, ces dispositions visent à

avoir son établissement principal dans un État membre lorsque son siège social se trouve dans cet État membre. 2. Un fournisseur de service numérique qui n'est pas établi dans l'Union mais fournit des services visés à l'annexe III à l'intérieur de l'Union désigne un représentant dans l'Union. Le représentant est établi dans l'un des États membres dans lesquels les services sont fournis. Le fournisseur de service numérique est considéré comme relevant de la compétence de l'État membre dans lequel le représentant est établi.	l'Union européenne et dont le siège social est situé sur le territoire national ou qui, n'étant pas établi dans l'Union européenne, ont désigné à cet effet un représentant sur le territoire national.	permettre à ces personnes de déterminer si elles sont dans le champ d'application de la présente directive.
CHAPITRE VI NORMALISATION ET NOTIFICATION VOLONTAIRE		
Art. 19. Normalisation 1. Afin de favoriser la convergence de la mise en œuvre de l'article 14, paragraphes 1 et 2, et de l'article 16, paragraphes 1 et 2, les États membres encouragent, sans imposer l'utilisation d'un type particulier de technologies ni créer de discrimination en faveur d'un tel type particulier de technologies, le recours à des normes et des spécifications européennes ou internationalement reconnues pour la sécurité des réseaux et des systèmes d'information. 2. L'ENISA, en collaboration avec les États membres, formule des avis et des lignes directrices relatives aux domaines techniques qui doivent être pris en considération en liaison avec le paragraphe 1 et relatives aux normes existantes, y compris les normes nationales des États membres, qui permettraient de couvrir ces domaines.		
Art. 20. Notification volontaire 1. Sans préjudice de l'article 3, les entités qui n'ont pas été identifiées en tant qu'opérateurs de services essentiels et qui ne sont pas des fournisseurs de service numérique peuvent notifier, à titre volontaire, les incidents ayant un impact significatif sur la continuité des services qu'elles fournissent. 2. Lorsqu'ils traitent des notifications, les États membres agissent conformément à la procédure énoncée à l'article 14. Les États membres peuvent traiter les notifications obligatoires en leur donnant la priorité par rapport aux notifications volontaires. Les notifications volontaires ne sont traitées que lorsque leur traitement ne fait pas peser de charge disproportionnée ou inutile sur les États membres concernés. Une notification volontaire n'a pas pour effet d'imposer à l'entité qui est à l'origine de		Des mesures de nature règlementaire permettront à l'opérateur non soumis à la directive de déclarer les incidents dont ils sont victimes de sorte à améliorer le niveau global de la cybersécurité.

la notification des obligations auxquelles elle n'aurait pas été soumise si elle n'avait pas procédé à ladite notification.		
CHAPITRE VII DISPOSITIONS FINALES		
Art. 21. (sanctions) : Les États membres fixent des règles relatives aux sanctions applicables en cas d'infraction aux dispositions nationales adoptées en vertu de la présente directive et prennent toutes les mesures nécessaires pour que ces règles soient appliquées. Les sanctions prévues sont effectives, proportionnées et dissuasives.	**Art. 9**. (opérateurs de services essentiels) Est puni d'une amende de 100 000 € le fait, pour les dirigeants des opérateurs mentionnés à l'article 5, de ne pas se conformer aux règles de sécurité mentionnées à l'article 6 et rappelées dans une mise en demeure, à l'expiration du délai défini par celle-ci. Est puni d'une amende de 75 000 € le fait, pour les mêmes personnes, de ne pas satisfaire à l'obligation de déclaration d'incident prévue au premier alinéa de l'article 7. Est puni d'une amende de 125 000 € le fait, pour les mêmes personnes, de faire obstacle aux opérations de contrôle mentionnées à l'article 8. **Art. 15.** (fournisseurs de services numériques) Est puni d'une amende de 75 000 € le fait, pour les dirigeants des fournisseurs de service numérique mentionnés à l'article 11, de ne pas prendre les mesures de sécurité nécessaires conformément aux dispositions de l'article 12 et mentionnées dans une mise en demeure, à l'expiration du délai défini par celle-ci.	Les sanctions sont proposées en cohérence avec celles prévues à l'article L. 1332-7 du code de la défense applicables aux opérateurs d'importance vitale. Toutefois, les montants des amendes sont ici plus faibles et différentiés selon les infractions.

	Est puni d'une amende de 50 000 € le fait, pour les mêmes personnes, de ne pas satisfaire aux obligations de déclaration d'incident ou d'information du public prévues à l'article 13. Est puni d'une amende de 100 000 € le fait, pour les mêmes personnes, de faire obstacle aux opérations de contrôle mentionnées à l'article 14.	
Art. 25. Transposition 1. Les États membres adoptent et publient, au plus tard le 9 mai 2018, les dispositions législatives, réglementaires et administratives nécessaires pour se conformer à la présente directive. Ils en informent immédiatement la Commission. Ils appliquent ces dispositions à partir du 10 mai 2018. Lorsque les États membres adoptent ces dispositions, celles-ci contiennent une référence à la présente directive ou sont accompagnées d'une telle référence lors de leur publication officielle. Les modalités de cette référence sont arrêtées par les États membres. 2. Les États membres communiquent à la Commission le texte des dispositions essentielles de droit interne qu'ils adoptent dans le domaine régi par la présente directive.	**TITRE V- DISPOSITIONS TRANSITOIRES** **Art. 22.** Les dispositions des chapitres Ier et III du titre Ier entrent en vigueur à compter d'une date définie par décret en Conseil d'Etat et au plus tard le 9 mai 2018. La désignation des opérateurs de services essentiels prévue au 1er alinéa de l'article 5 intervient au plus tard le 9 novembre 2018.	

ANNEXE III : TRANSPOSITION DE LA DÉCISION N° 1104/2011/UE DU 25 OCTOBRE 2011 DU PARLEMENT EUROPÉEN ET DU CONSEIL DU 25 OCTOBRE 2011 RELATIVE AUX MODALITES D'ACCES AU SERVICE PUBLIC REGLEMENTE OFFERT PAR LE SYSTEME MONDIAL DE RADIONAVIGATION PAR SATELLITE ISSU DU PROGRAMME GALILEO

Dispositions de la décision à transposer	**Normes de droit de l'Union également applicables / Normes de droit interne existantes portant déjà transposition de certaines dispositions de la décision**	**Nature juridique des nouvelles normes à adopter pour assurer l'entière transposition de la directive**	**Dispositions proposées**	**Observations (le cas échéant)**
DÉCISION N° 1104/2011/UE DU PARLEMENT EUROPÉEN ET DU CONSEIL du 25 octobre 2011 relative aux modalités d'accès au service public réglementé offert par le système mondial de radionavigation par satellite issu du programme Galileo			Article 20 Le Titre II du livre III de la deuxième partie du code de la défense est complété par un chapitre ainsi rédigé : « CHAPITRE III « SERVICE PUBLIC REGLEMENTE DE RADIONAVIGATION PAR SATELLITE [GALILEO]	L'intitulé du chapitre est issu de la formulation du titre de la décision n° 1104/2011/UE, qui emploie la notion de « service public réglementé » (celui-ci est réservé aux utilisateurs autorisés par les gouvernements, pour les applications sensibles qui exigent un niveau élevé de continuité du service et utilise des signaux robustes et cryptés).
Article premier - Objet La présente décision définit les modalités selon lesquelles les États membres, le Conseil, la Commission, le SEAE, les agences de l'Union, les pays tiers et les organisations internationales peuvent avoir accès au service public réglementé (PRS) offert par le système global de navigation par satellite issu du programme				

Galileo.				
Article 2 - Définitions Aux fins de la présente décision, on entend par: a) «usagers du PRS», les États membres, le Conseil, la Commission et le SEAE, ainsi que les agences de l'Union, les pays tiers et les organisations internationales, pour autant que ces agences, pays tiers et organisations aient été dûment autorisés; b) «utilisateurs du PRS», les personnes physiques ou morales dûment autorisées par un usager du PRS à détenir ou à utiliser un récepteur PRS.				
Article 3 – Principes généraux en matière d'accès au PRS : 1. Les États membres, le Conseil, la Commission et le SEAE ont le droit d'accéder au PRS de manière illimitée et ininterrompue dans toutes les parties du monde. 2. Il appartient à chaque État membre, au Conseil, à la Commission et au SEAE de décider s'ils ont recours au PRS dans les limites de leurs compétences respectives. 3. Chaque État membre qui a recours au PRS décide de manière indépendante, d'une part, des catégories de personnes		Instauration d'un régime d'autorisation par la loi Les modalités de regroupement des utilisateurs et de gestion des droits d'accès et des clés seront définies réglementairement.	« Section 1 « Activités contrôlées 3. « Art. L. 2323-1 - L'accès au service public réglementé offert par le système mondial de radionavigation par satellite issu du programme européen Galileo, (…) ne peuvent s'exercer qu'après autorisation délivrée par l'autorité administrative et sous son contrôle. Les autorisations délivrées en application du présent article peuvent être assorties de conditions ou de restrictions.	Exigence d'une autorisation administrative pour accéder au service public réglementé offert par le système mondial de radionavigation par satellite issu du programme européen Galileo (désigné

physiques résidant sur son territoire ou exerçant des fonctions officielles à l'étranger au nom de cet État membre et des catégories de personnes morales établies sur son territoire qui sont autorisées à être des utilisateurs du PRS et, d'autre part, des utilisations qui en sont faites, conformément à l'article 8 et aux points 1, i) et ii), de l'annexe. Ces utilisations peuvent comprendre des utilisations liées à la sécurité. Le Conseil, la Commission et le SEAE décident des catégories de leurs agents autorisées à être des utilisateurs du PRS, conformément à l'article 8 et aux points 1, i) et ii), de l'annexe. 4. Une agence de l'Union ne peut devenir un usager du PRS que dans la mesure où cela lui est nécessaire pour accomplir sa mission et selon les règles détaillées prévues par un accord administratif passé entre la Commission et l'agence concernée. 5. Un pays tiers ou une organisation internationale ne peut devenir un usager du PRS que si, conformément à la procédure prévue à l'article 218 du traité sur le fonctionnement de l'Union européenne, les deux accords suivants ont été conclus entre l'Union, d'une part, et le	**Décision 2014/496/PESC du Conseil du 22 juillet 2014 sur les aspects du déploiement, de l'exploitation et de l'utilisation du système mondial de navigation par satellite européen portant atteinte à la sécurité de l'Union européenne et abrogeant l'action commune 2004/552/PESC** Article 6 1. Conformément aux accords internationaux antérieurs conclus par l'Union ou par l'Union et ses États membres, y compris ceux ouvrant l'accès au PRS en application de l'article 3,			aussi par le sigle PRS, de l'anglais *public regulated service*). Chaque Etat a la faculté de décider de l'utilisation faite du PRS. Cela peut prendre la forme de conditions ou de restrictions dont les autorisations délivrées pourront être assorties.

pays tiers concerné ou l'organisation internationale concernée, d'autre part: a) un accord sur la sécurité des informations définissant le cadre d'échange et de protection des informations classifiées qui offre un degré de protection au moins équivalent à celui des États membres; b) un accord fixant les termes et conditions des modalités d'accès au PRS par ce pays tiers ou cette organisation internationale; cet accord pourrait notamment porter sur la fabrication, à certaines conditions, de récepteurs PRS, à l'exclusion des modules de sécurité.	paragraphe 5, de la décision n° 1104/2011/UE, le HR est compétent pour conclure des accords administratifs avec des États tiers en ce qui concerne la coopération dans le cadre de la présente décision. Ces accords sont soumis à l'approbation du Conseil statuant à l'unanimité.			
Article 4 -Application des règlements en matière de sécurité 1. Chaque État membre veille à ce que ses règlements nationaux en matière de sécurité assurent un niveau de protection des informations classifiées au moins équivalent à celui qui est garanti par les règles en matière de sécurité qui figurent à l'annexe de la décision 2001/844/CE, CECA, Euratom et par la décision 2011/292/UE et que ces règlements nationaux en matière de sécurité s'appliquent à ses utilisateurs du PRS et à toute	Règlement n° 1285/2003 **Article 17 - Application de la règlementation en matière d'informations classifiées** Dans les limites du présent règlement: a) chaque État membre veille à ce que sa réglementation nationale en matière de sécurité offre un niveau de protection des informations classifiées de l'UE équivalent à celui qui est prévu par les règles de sécurité qui figurent à l'annexe de la décision 2001/844/CE, CECA, Euratom et par les règles de sécurité du Conseil qui figurent dans les annexes de la			

personne physique résidant ou à toute personne morale établie sur son territoire qui traite des informations classifiées de l'UE relatives au PRS. 2. Les États membres informent sans délai la Commission de l'adoption des règlements nationaux en matière de sécurité visés au paragraphe 1. 3. S'il apparaît que des informations classifiées de l'UE relatives au PRS ont été divulguées à toute personne non autorisée à en recevoir, la Commission doit, en concertation étroite avec l'État membre concerné: a) informer l'autorité d'origine des données PRS classifiées; b) évaluer le préjudice potentiel causé aux intérêts de l'Union ou des États membres; c) notifier aux autorités compétentes le résultat de cette évaluation en l'assortissant d'une recommandation visant à remédier à la situation; dans ce cas, les autorités compétentes informent la Commission sans délai des mesures qu'elles prévoient de prendre ou qu'elles ont déjà prises, y compris les mesures visant à éviter que les faits ne se reproduisent, ainsi que des résultats de ces mesures; et d) informer le Parlement	décision 2013/488/UE; b) les États membres informent sans tarder la Commission de la réglementation nationale en matière de sécurité visée au point a);			

européen et le Conseil, comme il convient, de ces résultats.				
Article 5 – Autorité PRS responsable 1. Une autorité PRS responsable est désignée par: a) chaque État membre qui a recours au PRS et chaque État membre sur le territoire duquel une entité visée à l'article 7, paragraphe 1, est établie; dans les cas précités, l'autorité PRS responsable est établie sur le territoire de l'État membre concerné, qui notifie sans délai cette désignation à la Commission; b) le Conseil, la Commission et le SEAE, s'ils ont recours au PRS. Dans ce cas, l'agence du GNSS européen établie par le règlement (UE) n° 912/2010 (ci-après dénommée «agence du GNSS européen») peut être désignée comme autorité PRS responsable, selon des modalités appropriées; c) des agences de l'Union et des organisations internationales, conformément aux dispositions des accords visés à l'article 3, paragraphes 4 et 5. Dans ce cas, l'agence du GNSS européen peut être désignée comme autorité PRS responsable; d) des pays tiers, conformément aux dispositions des accords visés à l'article 3, paragraphe 5.	Article 14 du règlement n° 1285/2013 Conformément aux lignes directrices formulées par la Commission, l'agence du GNSS européen : (…) b) s'acquitte des tâches prévues à l'article 5 de la décision n° 1104/2011/UE et assiste la Commission conformément à l'article 8, paragraphe 6, de ladite décision	Désignation de l'autorité PRS responsable devra être inscrite dans un texte règlementaire		1. Autorité responsable en France est le SGDSN. Il a été désigné par une simple lettre notifiée à la Commission. Il conviendra de compléter l'article R* 1132-3 du code de la défense afin d'inscrire dans une norme cette désignation.

2. Les coûts de fonctionnement d'une autorité PRS responsable sont pris en charge par les usagers du PRS qui l'ont désignée. 3. Tout État membre qui n'a pas désigné d'autorité PRS responsable conformément au paragraphe 1, point a), désigne dans tous les cas un point de contact qui fournit l'aide nécessaire pour la notification de toute interférence électromagnétique potentiellement préjudiciable au PRS qui a été détectée. L'État membre concerné notifie sans tarder cette désignation à la Commission. 4. Chaque autorité PRS responsable veille à ce que l'utilisation du PRS soit conforme à l'article 8 et au point 1 de l'annexe et à ce que: a) les utilisateurs du PRS soient regroupés pour la gestion du PRS avec le CSSG; b) les droits d'accès au PRS pour chaque groupe ou utilisateur soient déterminés et gérés; c) les clés du PRS et d'autres informations classifiées connexes soient obtenues auprès du CSSG; d) les clés du PRS et d'autres informations classifiées connexes	Décision déléguée de la Commission du 15 septembre 2015 fixant les normes minimales communes	Missions incombant à l'autorité PRS. Les modalités de regroupement des utilisateurs et de gestion des droits d'accès et des clés seront définies réglementairement.	« Art. L. 2323-1 - L'accès au service public réglementé offert par le système mondial de radionavigation par satellite issu du programme européen Galileo,	2. en pratique, le SGDSN est un service du PM 3. sans objet, autorité désignée pour la France

soient distribuées aux utilisateurs; e) la sécurité des récepteurs et celle de la technologie et des informations classifiées connexes soient contrôlées et les risques évalués; f) soit établi un point de contact chargé de fournir l'aide nécessaire pour la notification de toute interférence électromagnétique potentiellement préjudiciable au PRS qui a été détectée. 5. L'autorité PRS responsable d'un État membre veille à ce qu'une entité établie sur le territoire de cet État membre ne puisse développer ou fabriquer des récepteurs PRS ou des modules de sécurité que si cette entité: a) a été dûment autorisée par le conseil d'homologation de sécurité conformément à l'article 11, paragraphe 2, du règlement (UE) no 912/2010; et b) se conforme à la fois aux décisions du conseil d'homologation de sécurité, à l'article 8 et au point 2 de l'annexe pour ce qui concerne le développement et la fabrication des récepteurs PRS ou des modules de sécurité, dans la mesure où ces dispositions portent sur ses activités.			le développement ou la fabrication de récepteurs ou de modules de sécurité conçus pour ce service et	

Toute autorisation prévue au présent paragraphe aux fins de la fabrication d'équipements fait l'objet d'un réexamen au moins tous les cinq ans. 6. S'agissant des activités de développement ou de fabrication visées au paragraphe 5 du présent article, ou dans le cas d'exportations en dehors de l'Union, l'autorité PRS responsable de l'État membre concerné joue le rôle d'interface pour les entités compétentes en matière de restrictions à l'exportation des équipements, de la technologie et des logiciels pertinents en ce qui concerne l'utilisation et le développement du PRS et la fabrication destinée à celui-ci, afin de garantir l'application des dispositions de l'article 9. 7. Les autorités PRS responsables sont reliées au CSSG conformément à l'article 8 et au point 4 de l'annexe. 8. Les paragraphes 4 et 7 s'entendent sans préjudice de la possibilité pour les États membres de déléguer d'un commun accord à un autre État membre certaines tâches spécifiques incombant à leur		Réexamen tous les 5 ans à prévoir - règlement	l'exportation d'équipements, de technologie ou de logiciels conçus pour ce service ne peuvent s'exercer qu'après autorisation délivrée par l'autorité administrative et sous son contrôle. Les autorisations délivrées en application du présent article peuvent être assorties de conditions ou de restrictions. Elles peuvent être abrogées, retirées, modifiées ou suspendues en cas de manquement du titulaire aux conditions spécifiées dans l'autorisation ou lorsque le respect des engagements internationaux de la France, la protection du service public réglementé ou celle des intérêts essentiels d'ordre public ou de sécurité publique le justifient	L'autorité administrative est tenue d'assurer un contrôle y compris postérieurement à la délivrance de l'autorisation , » .

autorité PRS responsable, à l'exclusion de toutes les tâches relatives à l'exercice de la souveraineté sur leurs territoires respectifs. Les tâches visées aux paragraphes 4 et 7, ainsi que celles visées au paragraphe 5, peuvent être effectuées en commun par les États membres. Les États membres concernés notifient sans délai à la Commission de telles mesures. 9. Une autorité PRS responsable peut demander l'assistance technique de l'agence du GNSS européen afin de s'acquitter des tâches qui lui incombent, selon des modalités spécifiques. Les États membres concernés notifient sans délai à la Commission de telles modalités. 10. Tous les trois ans, les autorités PRS responsables font rapport à la Commission et à l'agence du GNSS européen sur le respect des normes minimales communes. 11. Tous les trois ans, avec l'aide de l'agence du GNSS européen, la Commission fait rapport au Parlement européen et au Conseil sur le respect des normes minimales communes par les autorités PRS responsables, ainsi		Règlement		10. le considérant 25 de la décision indique : « Dès que le PRS est déclaré opérationnel, un mécanisme d'élaboration de rapports et d'évaluation devrait être mis en place

qu'à tout moment en cas de violation grave de ces normes. 12. Lorsqu'une autorité PRS responsable ne se conforme pas aux normes minimales communes énoncées à l'article 8, la Commission peut formuler une recommandation dans le respect du principe de subsidiarité et en concertation avec l'État membre concerné et, au besoin, après l'obtention d'informations spécifiques supplémentaires. Dans les trois mois suivant la formulation de la recommandation, l'autorité PRS responsable concernée soit se conforme à la recommandation de la Commission, soit réclame ou propose des modifications afin de se mettre en conformité avec les normes minimales communes et met ces modifications en oeuvre en accord avec la Commission. Si l'autorité PRS responsable concernée ne respecte toujours pas les normes minimales communes une fois la période de trois mois écoulée, la Commission en informe le Parlement européen et le Conseil et propose l'adoption de mesures appropriées.				
Article 6 -Rôle du CSSG (Centre de surveillance de la				

sécurité Galileo) Le CSSG fournit une interface opérationnelle entre les autorités PRS responsables, le Conseil ainsi que le haut représentant de l'Union pour les affaires étrangères et la politique de sécurité agissant au titre de l'action commune 2004/552/PESC et les centres de contrôle. Il informe la Commission de tout événement susceptible d'affecter le bon fonctionnement du PRS.				
Article 7 - Fabrication et sécurité des récepteurs et des modules de sécurité 1. Un État membre peut, sous réserve des exigences énoncées à l'article 5, paragraphe 5, confier à des entités établies sur son territoire ou sur le territoire d'un autre État membre la fabrication des récepteurs PRS ou des modules de sécurité associés. Le Conseil, la Commission ou le SEAE peuvent confier à des entités établies sur le territoire d'un État membre la fabrication des récepteurs PRS ou des modules de sécurité associés destinés à leur propre usage. 2. Le conseil d'homologation de sécurité peut à tout moment retirer à une entité mentionnée au paragraphe 1 du présent article l'autorisation qu'il lui a accordée			L. 2323-1 alinéa 1er le développement ou la fabrication de récepteurs ou de modules de sécurité conçus pour ce service (…) ne peuvent s'exercer qu'après autorisation délivrée par l'autorité administrative et sous son contrôle L. 2323-1 alinéa 2 « Les autorisations délivrées en application du présent article peuvent être assorties de conditions ou de restrictions. Elles peuvent être abrogées, retirées, modifiées ou suspendues en cas de manquement du titulaire aux conditions spécifiées dans l'autorisation ou lorsque le respect des engagements internationaux de la France, la protection du service public	

de fabriquer des récepteurs PRS ou des modules de sécurité associés si les mesures prévues à l'article 5, paragraphe 5, point b), ne sont pas respectées.			réglementé ou celle des intérêts essentiels d'ordre public ou de sécurité publique le justifient	
Article 8 - Normes minimales communes 1. Les normes minimales communes auxquelles doivent se conformer les autorités PRS responsables visées à l'article 5 portent sur les domaines énumérés à l'annexe. 2. La Commission est habilitée à adopter des actes délégués en conformité avec l'article 11 en ce qui concerne l'adoption des normes minimales communes dans les domaines énumérés à l'annexe et, le cas échéant, des modifications actualisant l'annexe pour tenir compte de l'évolution du programme Galileo, notamment sur le plan de la technologie, et des modifications des besoins en matière de sécurité. 3. Sur la base des normes minimales communes visées au paragraphe 2 du présent article, la Commission peut adopter les exigences techniques, lignes directrices et autres mesures nécessaires. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 12,	**Décision déléguée de la Commission du 15 septembre 2015** complétant la décision n° 1104/2011/UE en ce qui concerne les normes minimales communes auxquelles doivent se conformer les autorités PRS responsables Article 17 - : 1. Avant le transfert de biens PRS d'un Etat membre à un autre Etat membre, l'APR désignée par l'Etat membre à partir du territoire duquel doit avoir lieu le transfert vérifie que tant l'entité qui transfère les biens PRS que l'entité qui les reçoit appartiennent à l'une des catégories suivantes : a) une entité autorisée par le conseil d'homologation de sécurité conformément à l'article 5, paragraphe 5, point a), de la décision n° 1104/2011/UE ; b) une APR ; c) un utilisateur du PRS dûment autorisé à être associé au transfert par l'APR concernée. L'APR notifie aux autorités nationales compétentes son évaluation du respect de l'ensemble des conditions énumérées au premier alinéa. Le transfert de biens PRS entre Etats membres est autorisé par les autorités nationales compétentes, en conformité avec les mesures prises en application de la présente décision et les dispositions applicables du règlement (CE) n°		Art. L. 2323-2. – Tout transfert d'équipements, de technologie ou de logiciels conçus pour le service public réglementé offert par le système mondial de radionavigation par satellite issu du programme européen Galileo effectué depuis la France vers les autres Etats membres de l'Union européenne fait l'objet d'une déclaration à l'autorité administrative	Le contrôle des transferts intra-communautaires n'est pas prévu expressément par la décision n° 1104/2011/UE, mais seulement au stade de la décision déléguée adoptant les normes minimales communes prévues par ladite décision. Afin de permettre les vérifications requises par ces normes minimales communes, une déclaration à l'autorité administrative est prévue. Cette déclaration et cette vérification permettraient, le cas échéant, de bloquer un transfert non conforme, par une intervention de l'autorité administrative auprès de l'auteur du transfert établi en France.

paragraphe 2. 4. La Commission veille à ce que les dispositions nécessaires soient prises pour que les mesures visées aux paragraphes 2 et 3 soient respectées et à ce qu'il soit satisfait aux exigences relatives à la sécurité du PRS, de ses utilisateurs et de la technologie y afférente, en tenant pleinement compte de l'avis des experts. 5. Afin d'encourager le respect du présent article, la Commission facilite la tenue, une fois par an au moins, d'une réunion de toutes les autorités PRS responsables. 6. La Commission s'assure, avec l'aide des États membres et de l'agence du GNSS européen, que les autorités PRS responsables respectent les normes minimales communes, notamment en procédant à des audits ou des inspections.	428/2009 du Conseil. Article 14 du règlement n° 1285/2013 Conformément aux lignes directrices formulées par la Commission, l'agence du GNSS européen : (…) b) s'acquitte des tâches prévues à l'article 5 de la décision n° 1104/2011/UE et assiste la Commission conformément à l'article 8, paragraphe 6, de ladite décision			
Article 9 – Restrictions à l'exportation : Les exportations, en dehors de l'Union, d'équipements, de technologie ou de logiciels relatifs à l'utilisation et au développement du PRS et à la fabrication destinée à celui-ci ne sont autorisées que conformément à l'article 8 et au point 3 de l'annexe et au titre des accords visés à l'article 3, paragraphe 5, ou au titre des			L. 2323-1 alinéa 1er l'exportation d'équipements, de technologie ou de logiciels conçus pour ce service ne peuvent s'exercer qu'après autorisation délivrée par l'autorité administrative et sous son contrôle.	Exigence d'une autorisation administrative pour exporter des équipements, de la technologie ou des logiciels conçus pour le service public réglementé.

accords concernant les modalités d'hébergement et de fonctionnement des stations de référence.				
Article 10 – Application de l'action commune 2004/552/PESC : La présente décision est appliquée sans préjudice des mesures arrêtées en vertu de l'action commune 2004/552/PESC.	Règlement n° 1285/2013 Article 16 - Action commune Dans tous les cas où l'exploitation des systèmes peut porter atteinte à la sécurité de l'Union ou de ses États membres, les procédures prévues par l'action commune 2004/552/PESC sont applicables.			L'action commune 2004/552/PESC a été remplacée par la décision 2014/496/PESC du Conseil du 22 juillet 2014 sur les aspects du déploiement, de l'exploitation et de l'utilisation du système mondial de navigation par satellite européen portant atteinte à la sécurité de l'Union européenne et abrogeant l'action commune 2004/552/PESC. Cette décision est relative à la gestion opérationnelle des menaces, lorsque la situation internationale l'exige ou dans l'hypothèse d'une menace pesant sur l'exploitation du système Galileo.
Article 11 - Exercice de la délégation 1. Le pouvoir d'adopter des actes délégués conféré à la Commission est soumis aux conditions fixées au présent article. 2. Le pouvoir d'adopter des actes délégués visé à l'article 8, paragraphe 2, est conféré à la Commission pour une période de	Règlement n° 1285/2013 Article 13 – Sécurité des systèmes et de leur fonctionnement 2. Sans préjudice des articles 14 et 16 du présent règlement et de l'article 8 de la			

cinq ans à compter du 5 novembre 2011. La Commission élabore un rapport relatif à la délégation de pouvoir au plus tard neuf mois avant la fin de la période de cinq ans. 3. La délégation de pouvoir visée à l'article 8, paragraphe 2, peut être révoquée à tout moment par le Parlement européen ou le Conseil. La décision de révocation met fin à la délégation de pouvoir qui y est précisée. La révocation prend effet le jour suivant celui de la publication de ladite décision au *Journal officiel de l'Union européenne* ou à une date ultérieure qui est précisée dans ladite décision. Elle ne porte pas atteinte à la validité des actes délégués déjà en vigueur. 4. Aussitôt qu'elle adopte un acte délégué, la Commission le notifie au Parlement européen et au Conseil simultanément. 5. Un acte délégué adopté en vertu de l'article 8, paragraphe 2, n'entre en vigueur que si le Parlement européen ou le Conseil n'a pas exprimé d'objections dans un délai de deux mois à compter de la notification de cet acte au Parlement européen et au Conseil ou si, avant l'expiration de ce délai, le Parlement européen et le Conseil ont tous deux informé la Commission de	décision n° 1104/2011/UE, la Commission adopte des actes délégués en conformité avec l'article 35, établissant les objectifs de haut niveau nécessaires pour assurer la sécurité des programmes Galileo et EGNOS visée au paragraphe 1.			

leur intention de ne pas exprimer d'objections. Ce délai est prolongé de deux mois à l'initiative du Parlement européen ou du Conseil.				
Article 12 - Comité 1. La Commission est assistée par le comité institué par le règlement (CE) n o 683/2008. Ledit comité est un comité au sens du règlement (UE) n o 182/2011. 2. Lorsqu'il est fait référence au présent paragraphe, l'article 5 du règlement (UE) n o 182/2011 s'applique. Lorsque le comité n'émet aucun avis, la Commission n'adopte pas le projet d'acte d'exécution, et l'article 5, paragraphe 4, troisième alinéa, du règlement (UE) n o 182/2011 s'applique.				
Article 13 - Évaluation et rapport Au plus tard deux ans après que le PRS a été déclaré opérationnel, la Commission fait rapport au Parlement européen et au Conseil sur le fonctionnement adéquat et la pertinence des règles établies régissant l'accès au PRS et, le cas échéant, propose de modifier la présente décision en conséquence.				
Article 14 - Règles particulières pour la mise en œuvre du programme Galileo				

Nonobstant les autres dispositions de la présente décision, afin de garantir le bon fonctionnement du système issu du programme Galileo, les personnes et instances suivantes sont autorisées à accéder à la technologie PRS et à détenir ou utiliser des récepteurs PRS, sous réserve du respect des principes énoncés à l'article 8 et à l'annexe: a) la Commission, lorsqu'elle agit en tant que gestionnaire du programme Galileo; b) les exploitants du système issu du programme Galileo, aux fins strictes du respect du cahier des charges auquel ils doivent se conformer, selon les termes d'un arrangement spécifique conclu avec la Commission; c) l'agence du GNSS européen, pour lui permettre de s'acquitter des tâches qui lui sont confiées, selon les termes d'un arrangement spécifique conclu avec la Commission; d) l'Agence spatiale européenne, à de strictes fins de recherche, de développement et de déploiement de l'infrastructure, selon les termes d'un arrangement spécifique conclu avec la Commission.				

Article 15 – Sanctions : « Les États membres déterminent le régime des sanctions applicables aux violations des dispositions nationales adoptées en application de la présente décision. Les sanctions sont efficaces, proportionnées et dissuasives. »			« Section 2 « Sanctions pénales « Art. L. 2323-4 - Est puni d'une amende de 200 000 euros le fait de se livrer à une activité définie à l'article L. 2323-1 : « 1° sans autorisation ; « 2° sans respecter les conditions ou restrictions dont est assortie l'autorisation mentionnée à l'article L. 2323-1. « La tentative des délits prévus aux alinéas précédents est punie des mêmes peines. « Art. L. 2323-5. - Est punie d'une amende de 50 000 euros la méconnaissance de l'obligation prévue à l'article L. 2323-2. « Art. L. 2323-6. - I. – Les personnes physiques coupables de l'une des infractions prévues aux articles L. 2323-4 et L. 2323-5 encourent également les peines complémentaires suivantes : « 1° La confiscation, suivant les modalités prévues par l'article 131-21 du code pénal, de la chose qui a servi ou était destinée à commettre l'infraction ou de la chose qui en est le produit, à l'exception des objets susceptibles de restitution ; « 2° L'interdiction, suivant les modalités prévues par l'article 131-27 du code pénal et pour une durée de cinq ans au plus, d'exercer une fonction publique ou d'exercer l'activité professionnelle ou sociale	

			dans l'exercice ou à l'occasion de l'exercice de laquelle l'infraction a été commise. « 3° La fermeture, dans les conditions prévues par l'article 131-33 du code pénal et pour une durée de cinq ans au plus, des établissements ou de l'un ou de plusieurs des établissements de l'entreprise ayant servi à commettre les faits incriminés ; « 4° L'exclusion, dans les conditions prévues par l'article 131-34 du code pénal et pour une durée de cinq ans au plus, des marchés publics. « II. – Les personnes morales déclarées responsables pénalement, dans les conditions prévues par l'article 121-2 du code pénal, des infractions définies à la présente section encourent, outre l'amende suivant les modalités prévues par l'article 131-38 du code pénal, les peines prévues par les 1°, 2°, 4°, 5°, 8°, 9° et 12° de l'article 131-39 du même code. »	
Article 16 - Entrée en vigueur et application 1. La présente décision entre en vigueur le jour suivant celui de sa publication au *Journal officiel de l'Union européenne*. 2. Les États membres appliquent l'article 5 au plus tard le 6 novembre 2013.		Règlement pour désigner dans un texte le SGDSN		Echéance respectée par la France

CONSEIL D'ETAT

Séances du mardi 14 novembre 2017

Section de l'intérieur
Section de l'administration

N° 393665

EXTRAIT DU REGISTRE DES DELIBERATIONS

AVIS SUR UN PROJET DE LOI

portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité

NOR : INTX1728622L

1. Le Conseil d'Etat a été saisi le 18 octobre 2017 d'un projet de loi portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité. Cette saisine a été complétée par une saisine rectificative, reçue le 14 novembre 2017, portant sur l'étude d'impact.

2. Ce projet de loi, qui comprend vingt-deux articles, est organisé en cinq titres. Les trois premiers ont pour objet de transposer ou mettre en œuvre des directives ou décisions européennes :

- le titre I^{er} transpose la directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union ;

- le titre II transpose la directive (UE) 2017/853 du Parlement européen et du Conseil du 17 mai 2017 modifiant la directive 91/477/CEE du 18 juin 1991 du Conseil relative au contrôle de l'acquisition et de la détention d'armes ;

- le titre III met en œuvre la décision n° 1104/2011/UE du Parlement européen et du conseil du 25 octobre 2011 relative aux modalités d'accès au service public réglementé offert par le système mondial de radionavigation par satellite issu du programme Galileo et par la décision déléguée de la Commission du 15 septembre 2015 qui la complète.

Les titres IV et V sont relatifs, respectivement, à l'application outre-mer et aux dispositions transitoires.

3. L'étude d'impact du projet, dont la version modifiée reçue le 14 novembre 2017 intègre les compléments sollicités par les rapporteurs, comporte, pour l'essentiel, les éléments requis par l'article 8 de la loi organique n° 2009-403 du 15 avril 2009, pris pour l'application du troisième alinéa de l'article 39 de la Constitution.

Le Conseil d'Etat regrette néanmoins qu'elle ne comporte pas, pour le titre I^{er}, un tableau de transposition complet permettant de s'assurer non seulement de la fidélité à la directive des dispositions du projet de loi mais aussi de l'exhaustivité de l'exercice de transposition.

4. Au-delà de ces remarques liminaires, et outre des améliorations de rédaction qui s'expliquent d'elles-mêmes, ce projet de loi appelle, de la part du Conseil d'Etat, les observations suivantes.

En ce qui concerne les dispositions transposant la directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union

5. La directive du 6 juillet 2016 vise à la fois à établir un cadre communautaire de coopération entre les Etats membres en matière de cyber-sécurité, à renforcer leurs capacités en ce domaine et à instaurer un cadre réglementaire pour mieux protéger la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels et des fournisseurs de service numérique.

6. Le Conseil d'Etat constate que des dispositions législatives sont nécessaires pour assurer la transposition de la directive, en tant qu'elle prévoit d'imposer aux opérateurs de services essentiels et aux fournisseurs de service numérique de veiller à la sécurité de leurs réseaux et services d'information en les contraignant à identifier les risques qui les menacent et à y remédier, à notifier à l'autorité compétente les incidents graves survenus, à les soumettre, à leurs frais, à des contrôles sur place et sur pièce en habilitant les entités compétentes pour procéder à ces contrôles à accéder à des informations et installations éventuellement couvertes par le secret industriel ou commercial et d'édicter des sanctions en cas de méconnaissance de ces obligations. Des dispositions législatives sont également nécessaires pour permettre à l'Etat de communiquer à des tiers des informations couvertes par un secret et recueillies auprès de ces entreprises.

7. Le Gouvernement a fait le choix de ne pas codifier ces dispositions de transposition. Dans la mesure où l'objectif poursuivi par ces mesures est un objectif de sécurité et non, à proprement parler, de défense et au regard de l'état actuel de la structure du code de la sécurité intérieure, le Conseil d'Etat estime ce choix justifié.

8. Le Conseil d'Etat estime préférable de regrouper dans un même chapitre, placé en début de titre, les dispositions communes à la sécurité des réseaux et système d'information des opérateurs de services essentiels et des fournisseurs de service numérique. Il lui paraît nécessaire de les compléter en définissant les notions de « réseaux et systèmes d'information » et leur sécurité. Il juge également nécessaire de mieux préciser l'articulation entre, d'une part, les mesures visant à assurer les règles de cyber-sécurité applicables aux réseaux et systèmes d'information de ces entreprises issues de la directive et, d'autre part, celles prévues par d'autres régimes sectoriels de protection de la sécurité des systèmes d'information, et de soumettre les prestataires qui seront chargés de procéder aux contrôles de ces entreprises aux mêmes exigences de confidentialité que les services de l'Etat.

9. Le chapitre relatif à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels définit en termes généraux la notion de services essentiels afin d'encadrer le pouvoir règlementaire qui fixera la liste des secteurs d'activité qu'ils recouvrent, le Premier ministre étant ensuite chargé d'identifier chacun de ces opérateurs. Il confie au pouvoir règlementaire le soin de définir les règles de sécurité adaptées aux risques connus et applicables aux réseaux et systèmes d'information nécessaires à la fourniture de services essentiels par ces opérateurs. Il énonce les règles relatives à la prévention des incidents compromettant la sécurité de ces réseaux et systèmes d'information, aux mesures à prendre pour en limiter l'impact et aux obligations des opérateurs en matière de déclaration de ces incidents Il permet, en tant que de besoin, de rendre publiques des informations ainsi recueillies et de les communiquer aux autorités compétentes d'autres Etats membres concernés par l'incident. Il prévoit la possibilité de soumettre ces opérateurs à des contrôles sur place et sur pièce qui s'effectueront à leurs frais et habilite l'autorité ou les prestataires chargés d'effectuer ces contrôles à accéder à tout élément ou information utile pour vérifier le niveau de sécurité des réseaux et systèmes d'information

contrôlés. Enfin le projet instaure des dispositions pénales sanctionnant le non respect des obligations ainsi fixées.

Le Conseil d'Etat considère que, sous réserve des modifications qu'il y a apportées pour en préciser la portée, les dispositions de ce chapitre transposent convenablement la directive. Il note, en particulier, que l'article 3 de la directive autorise la sur-transposition à laquelle le projet se livre en imposant la notification des incidents « susceptibles d'avoir » un impact significatif et que les dispositions pénales proposées sont conformes aux principes constitutionnels qui gouvernent la définition des délits et des peines et de nature à mettre en œuvre les dispositions de l'article 21 de la directive qui prévoit l'instauration par les Etats membres de sanctions « *efficaces, proportionnées et dissuasives* ».

10. Le dernier chapitre de ce titre est relatif au régime de sécurité applicable aux réseaux et systèmes d'information des fournisseurs de service numérique. Le projet en définit les différentes composantes et le champ d'application conformément aux termes de la directive. Il reprend, en particulier, l'exclusion prévue par la directive au profit des micro-entreprises et des petites entreprises, dont il précise les seuils. Il soumet les fournisseurs de service numérique ainsi définis à des obligations de sécurité adaptées aux risques existants en leur prescrivant d'identifier les risques, de prendre les mesures nécessaires et de déclarer les incidents, ces informations pouvant, si nécessaire, être rendues publiques et communiquées aux autorités des autres Etats membres concernés. Il prévoit la possibilité de soumettre un fournisseur qui aurait méconnu l'une de ces obligations à des contrôles sur place et sur pièce qui s'effectueront à ses frais et habilite l'autorité ou les prestataires chargés d'effectuer ces contrôles à accéder aux réseaux et systèmes d'information contrôlés ainsi qu'aux informations utiles pour vérifier leur niveau de sécurité. Enfin, le projet instaure des sanctions pénales en cas de non respect par les dirigeants de ces entreprises des obligations ainsi fixées.

Le Conseil d'Etat considère que, sous réserve des modifications qu'il a apportées pour en préciser la portée ou éviter toute sur-transposition proscrite, s'agissant des dispositions en cause, par l'article 16 §10 de la directive, le projet procède également, sur ce point, à une transposition convenable.

En ce qui concerne les dispositions transposant la directive (UE) 2017/853 du Parlement européen et du Conseil du 17 mai 2017 modifiant la directive 91/477/CEE du 18 juin 1991 du Conseil relative au contrôle de l'acquisition et de la détention d'armes

11. Le Conseil d'Etat constate que l'essentiel de la transposition de la directive du 17 mai 2017 modifiant la directive du 18 juin 1991 relative au contrôle de l'acquisition et de la détention d'armes appelle des mesures relevant du domaine réglementaire, mais que six modifications nécessitent une transposition par voie législative. Ces modifications ne remettent pas en cause la classification des armes en quatre catégories (A : armes interdites ; B : armes soumises à autorisation ; C : armes soumises à déclaration ; D : armes dont la détention est libre) issue de la loi n° 2012-304 du 6 mars 2012 relative à l'établissement d'un contrôle des armes moderne, simplifié et préventif, mais conduisent, dans un but de renforcement de la sécurité publique, à un réaménagement du classement des armes dans ces différentes catégories.

12. La directive supprime la catégorie D des armes à feu : désormais, toutes les armes à feu devront relever, au moins, de la catégorie C, c'est-à-dire être soumises à une déclaration et non plus à un simple enregistrement. Une catégorie D d'armes pouvant être acquises et détenues librement pourra continuer d'exister dans les droits nationaux, mais cette catégorie ne pourra plus comporter d'armes à feu, hors le cas des armes historiques qui étaient et demeurent en dehors du champ d'application de la directive et de certaines des reproductions de ces armes historiques.

Le projet de loi procède aux modifications nécessaires dans les dispositions législatives du code de la sécurité intérieure et du code de la défense qui mentionnent la sous-catégorie des armes de catégorie D soumises à enregistrement, afin de supprimer toutes les références à l'enregistrement.

13. Jusqu'à sa modification par la directive de 2017, la directive de 1991 excluait de son champ d'application les « *armes antiques* » ou leurs reproductions. Se fondant sur le fait que « *les reproductions d'armes à feu anciennes n'ont pas la même importance ou le même intérêt historique et peuvent être construites en recourant aux techniques modernes susceptibles d'améliorer leur durabilité et leur précision* » (considérant n° 27 de la directive), la directive de 2017 fait entrer dans le champ d'application de la directive de 1991 les reproductions d'armes anciennes dont la durabilité et la précision sont améliorées par rapport à celles de l'arme reproduite. Si les armes historiques elles-mêmes peuvent demeurer dans la catégorie D redessinée, désormais limitée aux armes dont l'acquisition et la détention sont totalement libres, certaines de leurs reproductions devront désormais être classées, au moins, en catégorie C.

Le projet de loi modifie l'article L. 311-4 du code de la sécurité intérieure, qui dans sa rédaction actuelle classe les armes historiques et leurs reproductions en catégorie D, pour renvoyer le classement de ces armes à un décret en Conseil d'Etat, lequel devra, conformément, aux principes énoncés à l'article L. 311-2 du même code, classer ces armes en fonction de leur dangerosité ou, par dérogation, de leur calibre. Ce faisant, le projet permet, outre d'assurer une correcte transposition des dispositions de la directive, de rétablir un partage juridiquement plus exact des domaines de la loi et du règlement, le classement des armes dans les différentes catégories définies par le législateur ne relevant pas du domaine de la loi.

14. Les dispositions de la directive applicables avant la modification de 2017 faisaient obligation aux Etats membres de prévoir un contrôle administratif pour les armuriers. La directive de 2017 étend cette obligation aux courtiers d'armes, c'est-à-dire aux personnes qui exercent une activité d'intermédiaire dans les transactions portant sur les armes et ce, quelle que soit la catégorie d'armes sur lesquelles porte leur activité.

Aujourd'hui, en droit français, les courtiers ne sont soumis à un agrément de l'autorité administrative, en application de l'article L. 2332-1 du code de la défense, que si leur activité porte sur des armes des catégories A et B. Le projet modifie l'article L. 313-2 du code de la sécurité intérieure, qui prévoit l'agrément des armuriers, pour y ajouter l'activité des courtiers et ce, pour toutes les catégories d'armes dont l'acquisition et la détention sont soumises à des conditions (A, B ou C), conformément à la directive.

15. La directive de 2017, par des modifications apportées à l'annexe I de la directive de 1991, surclasse certaines armes semi-automatiques qui étaient jusqu'alors classées en catégorie B, c'est-à-dire soumises à autorisation, pour les faire passer en catégorie A, c'est-à-dire prohibées (sauf pour les forces de sécurité publique). Parallèlement, la directive ouvre aux Etats membres la possibilité de déroger, pour certaines catégories de personnes et d'usages déterminés et dans des conditions strictement encadrées, à la prohibition d'acquisition et de détention de certaines de ces armes surclassées.

Si le changement de catégorie des armes concernées par ce surclassement devra être opéré par le pouvoir réglementaire, le projet de loi doit néanmoins modifier les dispositions législatives du code de la sécurité intérieure pour adapter les conditions d'acquisition et de détention des armes précédemment classées en catégorie B et qui seront à l'avenir, classées en catégorie A.

16. La directive de 2017 a introduit dans la directive de 1991 un nouvel article 5 *ter* qui impose, pour les ventes d'armes à distance, une vérification soit par un armurier, soit par une

autorité publique, de l'identité et, si nécessaire, de l'autorisation d'acquisition dont il dispose. Cette vérification doit intervenir « *avant la livraison ou, au plus tard, au moment de la livraison* ». En pratique, cette disposition interdit – hormis pour les ventes à distance effectuées par des armuriers, qui étaient et demeurent possibles – la livraison au domicile de l'acheteur.

L'article L. 313-5 du code de la sécurité intérieure, dans sa rédaction actuelle, comporte déjà une interdiction de principe de la livraison à domicile des armes acquises par correspondance ou entre particuliers, mais prévoit la possibilité de dérogations pour certaines armes fixées par décret en Conseil d'Etat. Le pouvoir réglementaire a fait un usage large de cette faculté de prévoir des dérogations, puisque l'article R. 313-23 du même code autorise les livraisons d'armes à domicile pour toutes les catégories d'armes.

Le projet de loi modifie l'article L. 313-5 du code de la sécurité intérieure pour supprimer la possibilité, pour le pouvoir réglementaire, de déroger à l'interdiction de livraison des armes acquises par correspondance ou entre particuliers au domicile de l'acquéreur. La directive ouvre une option aux Etats membres entre une vérification de l'identité et de l'autorisation par une autorité publique et une vérification par un armurier ou courtier agréé. Le projet de loi écarte la possibilité que cette vérification soit faite par une autorité publique et ne retient que la possibilité d'une vérification par un armurier ou courtier agréé, ce que le Conseil d'Etat considère, sur le plan de la bonne administration, comme un choix approprié.

En prévoyant que « *La transaction est réputée parfaite à compter de la remise effective à l'acquéreur* », le projet de loi écarte la règle générale, prévue à l'article 1583 du code civil, selon laquelle une vente « *est parfaite entre les parties, et la propriété est acquise de droit à l'acheteur à l'égard du vendeur, dès qu'on est convenu de la chose et du prix, quoique la chose n'ait pas encore été livrée ni le prix payé* ». Le Conseil d'Etat estime que cette exception au principe du consensualisme est justifiée et nécessaire pour éviter tout litige sur la propriété, dans le cas où la vérification effectuée par l'armurier révélerait que l'acquéreur ne remplit pas les conditions légales pour lui permettre d'acheter l'arme : tant que l'arme n'aura pas été remise, par l'armurier, entre les mains de l'acquéreur, celui-ci n'en sera pas propriétaire.

17. Enfin, l'article 10 de la directive de 1991 est complété par celle de 2017 pour prévoir la possibilité, pour les armuriers et courtiers, de refuser légalement de conclure des transactions portant sur des munitions « *qu'ils pourraient raisonnablement considérer comme suspectes en raison de leur nature ou de leur échelle* », ainsi que l'obligation, pour ces mêmes professionnels, de signaler ces transactions suspectes aux autorités compétentes.

Le projet de loi crée dans le code de la sécurité intérieure un nouvel article L. 313-6 qui transpose cette disposition, en en élargissant délibérément le champ, au-delà des seules munitions, aux transactions d'armes. Le Conseil d'Etat estime ce choix justifié, sur le plan de la sécurité publique, car il serait paradoxal et inefficace de permettre aux armuriers et courtiers de refuser d'effectuer des transactions suspectes de munitions, sans leur donner la même possibilité pour les armes.

Le caractère « *raisonnablement* » suspect de la transaction et les conséquences que l'armurier ou le courtier sera en droit d'en tirer constitueront, pour ce dernier, un « *motif légitime* » lui permettant de refuser légalement de procéder à une vente ou de conclure tout autre contrat, sans pouvoir se voir reprocher un refus de vente qu'interdit, vis-à-vis d'un consommateur, l'article L. 121-11 du code de la consommation.

En ce qui concerne les dispositions mettant en œuvre la décision n° 1104/2011/UE du Parlement européen et du conseil du 25 octobre 2011 relative aux modalités d'accès au

service public réglementé offert par le système mondial de radionavigation par satellite issu du programme Galileo

18. Le programme Galileo est l'infrastructure européenne de radionavigation et de positionnement par satellite, conçue à des fins civiles. Il est régi par les dispositions du règlement (UE) n° 1285/2013 du Parlement européen et du Conseil du 11 décembre 2013 relatif à la mise en place et à l'exploitation des systèmes européens de radionavigation par satellite et abrogeant le règlement (CE) n° 876/2002 du Conseil et le règlement (CE) n° 683/2008 du Parlement européen et du Conseil, l'Union européenne. Aux termes de l'article 2 de ce règlement, le programme Galileo doit offrir cinq types de service dont « *un service public réglementé (PRS) réservé aux utilisateurs autorisés par les gouvernements, pour les applications sensibles qui exigent un niveau élevé de continuité du service, service qui utilise des signaux robustes et cryptés*. » La décision n° 1104/2011/UE définit les modalités d'accès au service public réglementé. Elle est complétée par une décision déléguée de la Commission du 15 septembre 2015 relative aux normes minimales communes auxquelles doivent se conformer les autorités responsables.

19. Pour assurer la mise en œuvre en droit interne des dispositions des deux décisions précitées, le projet de loi complète le titre II du livre III de la deuxième partie du code de la défense par un nouveau chapitre III intitulé « service public réglementé de radionavigation par satellite ». Bien que Galileo soit un programme civil, aucune exclusion dans les usages gouvernementaux du PRS n'est prévue et ces usages sont, en pratique, le fait des services en charge de la sécurité et de la défense. Le PRS s'adresse à des communautés d'utilisateurs relevant principalement des ministères régaliens et est destiné à des applications militaires. Le Conseil d'Etat estime donc que le choix de codification retenu par le Gouvernement est justifié.

20. Certaines des dispositions de la décision n° 1104/2011/UE étant inscrites à l'identique dans le règlement n° 1285/2013 précité, lequel est d'effet direct, le projet de loi ne comporte, à juste titre, aucune disposition destinée à les mettre en œuvre.

21. L'article 3 de la décision n° 1104/2011/UE dispose que les Etats membres décident de manière indépendante, d'une part, des catégories de personnes autorisées à utiliser le service public réglementé, d'autre part, des utilisations qui en sont faites dans le respect des normes minimales communes fixées par l'annexe de la décision et par la décision déléguée du 15 septembre 2015. Pour la mise en œuvre de ces dispositions, le projet de loi crée trois régimes d'autorisation préalable relatifs :

- à l'accès au service public réglementé ;

- au développement ou la fabrication de récepteurs ou de modules de sécurité conçus pour ce service ;

- et à l'exportation d'équipements, de technologie ou de logiciels conçus pour ce service.

Le projet prévoit que les autorisations délivrées pourront être assorties de conditions et qu'elles pourront être abrogées, retirées, modifiées ou suspendues dans les cas qu'il définit.

Le Conseil d'Etat estime que ce régime d'autorisation préalable et de contrôle est justifié et nécessaire compte tenu des enjeux liés à la sécurité du PRS.

22. Pour les transferts intracommunautaires des équipements PRS, le projet instaure un régime de déclaration. Il met ainsi en œuvre les dispositions inscrites à l'article 17 de la décision déléguée du 15 septembre 2015. Eu égard au principe de confiance réciproque, un régime plus souple qu'un régime d'autorisation est justifié.

23. Le projet de loi prévoit des dispositions pénales sanctionnant le non respect des obligations ainsi fixées aux utilisateurs, fabricants ou exportateurs du PRS. Le Conseil d'Etat estime que les sanctions pénales proposées sont de nature à mettre en œuvre les dispositions de

l'article 15 de la décision qui prévoit l'instauration par les Etats membres de sanctions « *efficaces, proportionnées et dissuasives* ».

Le Conseil d'Etat rappelle que relève du domaine réservé à la loi par l'article 34 de la Constitution la désignation des agents habilités à rechercher et constater des infractions pénales. Il prend acte de la volonté du Gouvernement de ne pas attribuer de pouvoir de police judiciaire à des agents de l'administration. Le dispositif conserve son efficacité dans la mesure où les agents en capacité technique de constater des manquements doivent, en application des dispositions du second alinéa de l'article 40 du code de procédure pénale, en donner avis au procureur de la République.

24. Le Conseil d'Etat prend acte de ce que les modalités de mise en œuvre des normes minimales communes seront définies réglementairement. Il regrette toutefois que le Gouvernement n'ait pas été en mesure de communiquer le projet de décret qui sera pris pour l'application des dispositions du titre III, ce qui aurait permis de s'assurer d'une mise en œuvre complète de la décision. Il précise que la désignation de l'autorité responsable, qui résulte d'une lettre notifiée à la Commission conformément aux dispositions du *a* du paragraphe 1 de l'article 5 de la décision n° 1104/2011/UE, doit faire l'objet d'une inscription dans un texte réglementaire afin d'assurer l'intelligibilité des dispositions mettant en œuvre la décision.

25. Enfin, le projet de loi prévoit l'articulation des dispositions introduites dans le code de la défense relatives au contrôle des exportations du matériel et des technologies liés au PRS avec les dispositions ayant le même objet pour les biens à double usage et les matériels de guerre. Le Conseil d'Etat estime cette précision opportune dans la mesure où certains biens sont susceptibles de relever de deux régimes.

En ce qui concerne l'application outre-mer de ces dispositions

26. Le Gouvernement considère que, sous réserve des articles L. 2323-2 et L. 2323-5 du code de la défense, les dispositions de ces trois titres, qui intéressent la sécurité publique, ainsi que celles du titre V relatif aux dispositions transitoires, s'appliquent sur tout le territoire de la République, sous réserve d'une modification de coordination pour une disposition d'adaptation du titre II applicable en Nouvelle-Calédonie et d'une grille de lecture des dispositions qui renvoient à des actes de l'Union européenne pour leur application dans les collectivités où ces actes ne sont pas applicables.

Le Conseil d'Etat partage cette analyse.

En ce qui concerne les dispositions transitoires

27. Les chapitres I^er^ et III du titre I^er^ nécessitent, pour entrer en vigueur, des décrets d'application ainsi que des actes d'identification pour certaines dispositions. Le projet précise que leur entrée en vigueur interviendra, selon les cas, aux dates que prévoiront ces décrets ou à la date des actes d'identification des opérateurs de services essentiels et au plus tard aux dates limites de transposition fixées par chaque directive.

Ce projet de loi a été délibéré et adopté par le Conseil d'Etat (section de l'intérieur et section de l'administration) dans ses séances du 14 novembre 2017.