N° 554

ASSEMBLÉE NATIONALE

CONSTITUTION DU 4 OCTOBRE 1958

QUINZIÈME LÉGISLATURE

Enregistré à la Présidence de l'Assemblée nationale le 17 janvier 2018

RAPPORT

FAIT

AU NOM DE LA COMMISSION DES LOIS CONSTITUTIONNELLES, DE LA LÉGISLATION ET DE L'ADMINISTRATION GÉNÉRALE DE LA RÉPUBLIQUE, SUR LE PROJET DE LOI, ADOPTÉ PAR LE SÉNAT APRÈS ENGAGEMENT DE LA PROCÉDURE ACCÉLÉRÉE,

portant diverses **dispositions** *d'***adaptation** *au* **droit** *de l'***Union européenne** *dans le* **domaine** *de la* **sécurité** (n° 530),

PAR M. CHRISTOPHE EUZET
Député

Voir les numéros :

Sénat : **105**, **161**, **162** et T.A. **34** (2017-2018)

SOMMAIRE

___

PAGES

MESDAMES, MESSIEURS,

Le présent projet de loi a été présenté en Conseil des ministres le 22 novembre 2017 et adopté par le Sénat le 19 décembre, après engagement de la procédure accélérée.

Il s'agit d'un texte d'adaptation au droit de l'Union européenne, ayant pour objet la transposition de deux directives relatives, respectivement, à la cybersécurité de certains opérateurs essentiels au fonctionnement de l'économie et au contrôle de l'acquisition et de la détention d'armes. Il tire par ailleurs les conséquences d'une décision du Parlement européen et du Consel relative au système mondial de radionavigation par satellite issu du programme Galileo.

Le *titre I*^{er} du projet de loi (articles 1er à 15) a pour objectif 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. Il transpose, ce faisant, en 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, dite directive « *NIS* ».

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.

Les *titres IV* (article 23) et *V* (article 24) visent respectivement à permettre l'application sur l'ensemble du territoire de la République du présent projet de loi et à

prévoir les mesures transitoires rendues nécessaire par le report de l'entrée en vigueur de certaines de ses dispositions.

L'examen de ce projet de loi au Sénat a permis de préciser la rédaction de certaines dispositions mais n'a pas modifié son équilibre général, qui fait l'objet d'un relatif consensus. Votre rapporteur s'est également inscrit dans cette démarche.

I. LA CYBERSÉCURITÉ : UN ENJEU ÉCONOMIQUE MAJEUR

A. UNE MENACE CROISSANTE AUX GRAVES CONSÉQUENCES ÉCONOMIQUES

L'ensemble des secteurs d'activité sont susceptibles de faire l'objet d'une attaque informatique d'envergure, dont l'impact peut aller jusqu'à la paralysie de pans entiers de l'économie. Les exemples récents ne manquent pas, deux cyber-attaques de grande ampleur au moins ayant eu lieu pour la seule année 2017. La première est « *Wannacry* », en mai, qui a bloqué les ordinateurs de grandes entreprises et de services publics d'une centaine de pays. Ses victimes sont aussi diverses que le service de santé britannique, des grandes entreprises comme Renault et FedEx, l'opérateur de télécom espagnol Telefonica ou encore la compagnie ferroviaire allemande Deutsche Bahn. La seconde est « *NotPetya* » en juin, qui a affecté des centaines de milliers d'ordinateurs et qui, en France, a notamment touché l'entreprise Saint Gobain.

Différentes études pointent en outre l'augmentation rapide des coûts induits par les cyber-incidents. Ceux-ci correspondent aux coûts liés à l'indisponibilité et la reconstruction des systèmes d'information mais il ne faut pas non plus négliger que des dommages collatéraux, plus difficilement estimables, peuvent également être causés par de telles attaques : l'atteinte à l'image, la perte de marchés ou encore le vol d'informations sensibles.

L'agence européenne pour la sécurité des réseaux (ENISA) a récemment produit une analyse synthétisant les résultats de plusieurs études sur les coûts économiques des cyber-incidents et qui retenait les chiffres suivants [(1)] :

– le coût global des incidents cybernétiques atteindrait ainsi 1,6 % du PIB en Allemagne et 0,41 % au niveau de l'Union européenne ;

– le coût annuel moyen pour une entreprise britannique, allemande ou française serait estimé dans une fourchette comprise entre quelques centaines de milliers et une vingtaine de millions d'euros ;

– une étude chiffre le coût mondial dans une fourchette allant de 330 à 506 milliards d'euros.

Comme le souligne l'étude d'impact associée au projet de loi, dans le cadre des interventions que l'agence nationale de la sécurité des systèmes d'information

(1) The cost of incidents affecting CIIs *(disponible sur le site internet de l'ENISA).*

(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 compris entre **quelques millions et quelques dizaines de millions d'euros pour une seule cyber-attaque réussie**. À titre d'exemple, 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.

B. LA FRANCE, UN PAYS PIONNIER EN MATIÈRE DE CYBERSÉCURITÉ

Dès 2008, le Livre blanc sur la défense et la sécurité nationale a identifié les attaques contre les systèmes d'information comme l'une des principales menaces qui pèsent sur notre défense et notre sécurité. Pour y faire face, l'article 22 de la loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale a imposé aux opérateurs dits « *d'importance vitale* » le renforcement de la sécurité des systèmes d'information qu'ils exploitent. Ces obligations comprennent en particulier la déclaration d'incidents, la mise en œuvre d'un socle de règles de sécurité et le recours à des produits et à des prestataires de détection qualifiés.

La France dispose par ailleurs déjà d'une autorité nationale compétente en matière de sécurité des réseaux et des systèmes d'information. En effet, l'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. À 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 ;

– coordonner l'action gouvernementale dans le cadre des orientations fixées par le Premier ministre en matière de défense des systèmes d'information ;

– proposer les mesures de protection des systèmes d'information ;

– mener des inspections des systèmes des services de l'Etat et des opérateurs d'importance vitale ;

– participer aux négociations internationales et assurer la liaison avec ses homologues étrangers.

Elle assure enfin une fonction de centre de réponse et de traitement des incidents de sécurité (CSIRT).

C. LA DIRECTIVE « *NIS* »

S'inscrivant dans la logique de 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 au début de l'année 2013 [(2)] et adoptée le 6 juillet 2016. Communément appelée directive « *NIS* », elle a été publiée au *Journal officiel de l'Union européenne* le 19 juillet 2016 et doit être transposée d'ici au 9 mai 2018.

La directive a été prise sur le fondement de l'article 114 du Traité sur le fonctionnement de l'Union Européenne en raison du rôle majeur joué par la résilience des réseaux et systèmes informatiques dans le fonctionnement du marché intérieur. Compte tenu de la dimension transnationale des incidents et des risques de cyber-sécurité, la Commission européenne a estimé opportun de développer une action coordonnée au niveau de l'Union, dans le respect du principe de subsidiarité.

Il s'agit de la première initiative de l'Union européenne visant à légiférer de façon globale dans le champ de la cyber-sécurité par le renforcement de la résilience des réseaux et des systèmes d'information des infrastructures critiques. Cette résilience peut se définir 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.

Structurée autour de quatre axes, la directive prévoit :

– le renforcement des capacités des États membres en matière de cyber-sécurité (chapitre II). Ceux–ci doivent notamment se doter d'autorités nationales compétentes en matière de cyber-sécurité, d'équipes nationales de réponse aux incidents informatiques – les CSIRT – et de stratégies nationales de cyber-sécurité ;

– l'établissement d'un cadre de coopération volontaire entre les États membres (chapitre III) ;

– 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). 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). L'annexe III de la directive précise les types de services numériques concernés.

---

(1) Document COM(2010) 245 final du 19.5.2010.

(2) Document COM(2013) 48 final du 7.2.2013.

D. LE PROJET DE LOI DE TRANSPOSITION A ÉTÉ PRÉCISÉ PAR L'EXAMEN AU SÉNAT ET PAR VOTRE COMMISSION

Le titre I[er] du projet de loi (**articles 1[er] à 15**) transpose en 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, dite directive « *NIS* ». Il n'a fait l'objet, au Sénat comme en commission des Lois à l'Assemblée nationale, que de modifications de précision.

Le chapitre I[er] fixe les dispositions communes aux opérateurs de services essentiels (OSE) au fonctionnement de l'économie et aux fournisseurs de service numérique (FSN).

L'**article 1[er]** définit les notions de « *réseaux et systèmes d'information* » et de « *sécurité des systèmes d'information* ».

L'**article 2** précise le champ d'application des dispositions du titre I[er] en excluant du périmètre du projet de loi les réseaux et systèmes d'information déjà soumis, en application de normes européennes sectorielles, à des exigences en matière de sécurité des systèmes d'information, dès lors que ces exigences sont au moins équivalentes à celles créées par la nouvelle réglementation.

L'**article 3** précise les règles de confidentialité s'imposant à l'administration et aux prestataires de services habilités dans le cadre des activités exercées en application des dispositions du projet de loi.

L'**article 4** renvoie à un décret les modalités d'application du titre I[er].

Le chapitre II édicte les dispositions relatives à la sécurité des réseaux et systèmes d'information des OSE.

L'**article 5** précise la notion d'OSE et fixe les modalités de leur désignation.

L'**article 6** détermine le régime d'obligations applicable aux OSE en matière de sécurité des réseaux et systèmes d'information.

Lors de l'examen par la commission des Lois, votre rapporteur a présenté un amendement visant à préciser dans la loi la nature des règles de sécurité prévues à cet article afin de prendre en compte les remarques exprimées par le Sénat.

L'**article 7** introduit une obligation de signalement à l'ANSSI de certains incidents et fixe les conditions dans lesquelles l'administration est autorisée à communiquer sur un tel incident.

L'**article 8** prévoit la possibilité pour l'administration d'effectuer ou de faire pratiquer des contrôles auprès des OSE ainsi que la mise en place d'un pouvoir d'injonction à leur encontre.

L'**article 9** détermine les sanctions pénales encourues par les OSE en cas de manquement aux obligations fixées par le projet de loi.

Le chapitre III fixe les dispositions relatives à la sécurité des réseaux et des systèmes d'information des FSN.

L'**article 10** définit les notions de service numérique et de FSN.

L'**article 11** précise le champ d'application des dispositions prévues par le chapitre III.

L'**article 12** détermine les obligations s'imposant aux FSN.

L'**article 13** prévoit, à l'égard des FSN, une obligation de signalement de tout incident affectant les réseaux et systèmes d'information et un encadrement des conditions de la publicité donnée à ces incidents.

L'**article 14** détermine les modalités de contrôle des obligations imposées aux FSN en matière de sécurité des réseaux et systèmes d'information.

L'**article 15** détermine le régime de sanctions pénales applicable aux FSN en cas de manquement à leurs obligations.

II. UN CONTRÔLE ACCRU SUR L'ACQUISITION ET LA DÉTENTION D'ARMES

A. UNE PRÉOCCUPATION ANCIENNE

Dès 1991, l'Union européenne a poursuivi l'ambition d'**harmoniser les règles** applicables sur son territoire en matière d'acquisition et de détention d'arme à feu (1). Ses stipulations constituaient les premières exigences minimales auxquelles devaient satisfaire les États membres pour améliorer la sécurité de tous.

La persistance, aux frontières de l'Union européenne, de conflits armés dans les Balkans a justifié le maintien de l'objectif d'un contrôle des armes au sommet de l'agenda politique de l'Union européenne. La directive de 1991 a connu une première révision en 2008 (2) tandis que divers textes complémentaires d'exécution étaient édictés (3). Le droit international connaissait dans le même temps une progression

---

(1) Directive 91/477/CEE du Conseil du 18 juin 1991 relative au contrôle de l'acquisition et de la détention d'armes.

(2) Directive 2008/51/CE du Parlement européen et du Conseil du 21 mai 2008 modifiant la directive 91/477/CEE du Conseil du 18 juin 1991 relative au contrôle de l'acquisition et de la détention d'armes.

(3) Règlement (UE) n° 258/2012 du Parlement européen et du Conseil du 14 mars 2012 portant application de l'article 10 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 (protocole relatif aux armes à feu) et instaurant des autorisations d'exportation, ainsi que des mesures concernant l'importation et le transit d'armes à feu, de leurs pièces, éléments et munitions ; règlement d'exécution (UE) n° 2015/2403 de la Commission du 15 décembre 2015 établissant des lignes directrices communes concernant les normes et techniques de neutralisation en vue de garantir que les armes à feu neutralisées sont rendues irréversiblement inopérantes.

significative à l'initiative de l'Organisation des Nations unies, qui adoptait également en 2001 des règles contraignantes (1).

Les principes guidant l'action de la Commission européenne en matière de contrôle des armes à feu ont été formalisés dans une communication sur « *Les armes à feu et la sécurité intérieure dans l'Union européenne : protéger les citoyens et déjouer les trafics illicites* » (2). Comme les directives de 1991 et 2008, cette stratégie visait à la fois à encadrer le régime juridique des armes à feu et à préserver leur marché licite.

B. UNE RÉPONSE AUX ATTAQUES TERRORISTES DE 2015

Au lendemain des **attentats de Paris de janvier 2015**, la France a fait connaître son intérêt pour un nouveau renforcement du régime d'acquisition et de détention des armes à feu. La « **Déclaration de Paris** » n° 5322/15 du 11 janvier 2015 dans laquelle, à la suite immédiate de la vague d'attentats qui venait de frapper notre pays, les ministres de l'intérieur et de la justice de l'Union européenne ont notamment affirmé leur détermination à lutter contre la circulation illégale d'armes à feu sur le territoire de l'Union.

La Commission européenne a pris en compte cet objectif en complétant sa stratégie de sécurité par une **nouvelle communication**, le 28 avril 2015 (3). Les orientations de cette communication confèrent une priorité à la définition d'une approche commune en matière de neutralisation des armes à feu afin d'empêcher les criminels de les réactiver et de les utiliser, et, surtout, appellent à un réexamen des règles existantes afin d'améliorer le partage d'informations, la traçabilité et le marquage. Elles reprennent les préconisations formulées à l'occasion de l'évaluation des règles alors en vigueur (4).

La révision de la directive proposée le 18 novembre 2015 (5) se voulait un **changement de philosophie** : contrairement aux considérations retenues en 1991 et 2008, il n'était plus question d'appréhender les armes à feu comme de simples biens manufacturés d'usage courant dont la commercialisation sans entrave devait être assurée dans le Marché commun. **La sécurité des personnes devait primer sur la fluidité du commerce légal**.

---

(1) 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, adopté par la résolution de l'Assemblée générale 55/25 du 31 mai 2001.

(2) Communication de la Commission au Conseil et au Parlement européen (COM(2013) 716 final), Les armes à feu et la sécurité intérieure dans l'Union européenne : protéger les citoyens et déjouer les trafics illicites, *21 octobre 2013.*

(3) Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions COM(2015) 185 final, Le programme européen en matière de sécurité, *28 avril 2015.*

(4) Évaluation REFIT de la directive 91/477/CE du Conseil du 18 juin 1991 relative au contrôle de l'acquisition et de la détention d'armes, COM(2015) 751 final, 18 novembre 2015.

(5) Proposition de Directive du Parlement européen et du Conseil modifiant la directive 91/477/CEE du Conseil relative au contrôle de l'acquisition et de la détention d'armes, COM(2015) 750 final.

Le caractère suspect de certaines transactions légales avait été identifié ; leur lien avec le banditisme et le terrorisme établi. Des armes mises sur le marché en tant qu'armes « à blanc » n'avaient subi qu'une transformation réversible et pouvaient facilement redevenir létales. Lors des attentats de janvier 2015, un terroriste a utilisé deux fusils d'assaut acquis comme armes d'expansion acoustique puis reconditionnées.

C. LA DIRECTIVE « ARMES À FEU »

La proposition de révision des règles européennes en matière d'acquisition et de détention d'armes a reçu le soutien de l'Assemblée nationale (1). Elle est devenu la **directive (UE) 2017/853 du 17 mai 2017**, dont le titre II du présent projet de loi a vocation à assurer la transposition.

Comme l'a noté le rapporteur du Sénat, cette directive comporte « *principalement des mesures qui visent à* ***mieux encadrer les régimes légaux*** *d'acquisition et de détention des armes à feu, d'une part en durcissant les règles applicables pour les armes considérées comme les plus dangereuses, d'autre part en sécurisant les conditions de vente des armes à feu* » (2). Certes, il est possible de déplorer que ces dispositions affectent les acquéreurs et détenteurs d'armes respectueux des lois et règlements, quand les menaces sur la sécurité publique sont essentiellement le fait d'individus qui recourent à des circuits d'approvisionnement illicites, en marge des voies légales, et qui échapperont très largement à la réglementation prévue par la directive. Toutefois, la répression du marché noir et des trafics d'armes relève de l'investigation policière et judiciaire, non de la législation et des pratiques administratives. Il importait que le législateur agisse dans son champ de compétence, ce qui est bien le cas avec le présent projet de loi.

D. DES ADAPTATIONS LÉGISLATIVES PONCTUELLES

Comme le relève l'étude d'impact associée au projet de loi, la transposition de la directive du 17 mai 2017 sera **principalement mise en œuvre par voie réglementaire**. Le renforcement des règles de marquage et d'enregistrement des armes, les modalités de tenue des traitements de données les concernant, le contrôle des armes tirant des munitions à blanc et les dispositions en matière de stockage des armes sont, en effet, du ressort du Gouvernement.

Les prescriptions de la directive relevant du domaine législatif font l'objet du **titre II du projet de loi**.

Les **articles 16 et 17** tirent les conséquences de la suppression, en droit européen, de la catégorie D des armes à feu, qui a pour effet la disparition de la

---

(1) Résolution sur la proposition de directive du Parlement et du Conseil relative aux armes à feu, considérée comme définitive en application de l'article 151-7 du Règlement par l'Assemblée nationale le 11 juin 2016 , TA n° 751.

(2) Rapport n° 161 de M. Philippe Bonnecarrère à la commission des Lois sur le projet de loi portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité, 13 décembre 2017.

catégorie D1 en droit national. Le passage en catégorie A de certaines armes semi-automatiques est également prévu.

L'**article 18** encadre les ventes d'armes et de munitions. Il étend aux courtiers le régime légal des armuriers. Il prévoit une vérification de l'identité des acheteurs, y compris lors des ventes à distance, par correspondance ou entre particuliers. Il autorise armuriers et courtiers à refuser une vente considérée comme suspecte.

Les **articles 19, 20, 21 et 21 *bis*** procèdent à des coordinations dans le code de la sécurité intérieure, le code de la défense et la loi n° 55-385 du 3 avril 1955 relative à l'état d'urgence.

E. UN DISPOSITIF APPROUVÉ PAR VOTRE COMMISSION

Comme le Sénat, la commission des Lois a principalement apporté au projet de loi des améliorations rédactionnelles et formelles.

Elle a pris l'initiative, sur proposition du rapporteur, de réprimer la tentative d'acquisition ou de cession illégale d'armes de catégorie C des peines déjà prévues pour leur acquisition ou leur cession effective. Cette évolution permettra à la France de **ratifier sans réserve le Protocole des Nations unies sur les armes à feu**. Elle entre parfaitement dans le périmètre du projet de loi et de la directive qu'il transpose, l'un et l'autre prévoyant des mesures répressives pour le trafic d'armes.

Enfin, la Commission s'est opposée au Sénat quant au **classement des armes et matériels historiques et de collection ainsi que leurs reproductions**. Alors que le Sénat avait souhaité procéder par la loi à un classement en catégorie D, la Commission a privilégié l'analyse du Gouvernement et du Conseil d'État selon laquelle un tel classement relevait du domaine réglementaire et non de l'intervention du législateur.

III. L'ACCÈS SÉCURISÉ AUX SERVICES DU PROGRAMME GALILEO

Le **programme de radionavigation par satellite Galileo** a été lancé par l'Union européenne en 1999. L'exploitation des services de base a commencé en 2016. Le déploiement du programme doit s'achever en 2020, date à laquelle l'ensemble des services seront disponibles.

Le système Galileo offrira, à terme, trois services distincts : le premier accessible à tous et **gratuit**, le deuxième **commercial**, le troisième **réglementé** et sécurisé pour un usage restreint (SPR pour « service public réservé »).

Le SPR est adapté aux applications les plus sensibles, qui exigent la plus grande fiabilité et une continuité de service maximale. Employé aux fins de sécurité publique et d'intérêt général, il sera donc **réservé à un nombre restreint d'utilisateurs**, parmi lesquels les institutions de l'Union européenne et les États membres, ce qui justifie un **contrôle rigoureux pour son accès**.

Les modalités d'accès au SPR et leur contrôle **relève des États membres**, conformément à 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. Sont notamment prévues les sanctions pénales à mettre en œuvre en cas d'infraction aux règles de sécurité qui garantissent l'intégrité du SPR. La transposition de ces dispositions dans le droit national **conditionne l'accès** des États membres au service public réglementé.

Le titre III du projet de loi, composé d'un unique **article 22,** modifie le code de la défense pour le **mettre en conformité** avec la décision du 25 octobre 2011.

Eu égard à la précision de la décision précitée, le législateur dispose d'une très faible latitude d'interprétation pour sa transposition. Tant le Sénat que la commission des Lois n'ont donc **pas modifié la rédaction de l'article 22** proposée par le Gouvernement.

DISCUSSION GÉNÉRALE

Lors de sa réunion du mercredi 17 janvier 2018, la commission des Lois examine le projet de loi portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité (n° 530) (M. Christophe Euzet, rapporteur) adopté par le Sénat après engagement de la procédure accélérée.

M. Christophe Euzet, rapporteur. Le texte que nous examinons aujourd'hui vise à transposer une série de prescriptions européennes. C'est un ensemble relativement hétérogène puisqu'il s'agit de transcrire dans notre droit deux directives de 2016 et de 2017, et de tirer les conséquences d'une décision de 2011. Ces dispositions peuvent être rassemblées sous le thème de la sécurité.

Il s'agit d'abord de transposer la directive (UE) 2016/1148 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union, autrement dit à lutter contre la cybercriminalité au niveau européen et à garantir un niveau de sécurité élevé des réseaux et systèmes d'information des opérateurs de services dits essentiels – sur lesquels je reviendrai dans un instant.

Il s'agit ensuite de transposer la directive modifiant la directive 1104/2011/UE relative au contrôle de l'acquisition et de la détention d'armes en mettant en place un système de contrôle de l'acquisition et de la détention des armes à feu, ce qui se traduit par un durcissement de la législation autour de ce socle commun.

Il s'agit enfin de tirer les conséquences de la décision européenne relative au fonctionnement du système mondial de radionavigation par satellite issu du programme GALILEO.

Ce projet de loi est assez intéressant, pour peu que l'on accepte de « payer un droit d'entrée » pour en comprendre les subtilités techniques… Mais c'est aussi un exercice relativement contraint, comme à chaque fois qu'il s'agit de transposer le droit européen : il faut échapper au double écueil de la surtransposition, que nous essayons de plus en plus systématiquement d'éviter, et d'une sous-transposition répréhensible au regard de nos engagements européens.

Ce texte a été examiné par le Sénat en première lecture, qui l'a amendé sur un plan technique et de façon constructive ; c'est la raison pour laquelle nous vous proposerons de conserver la plupart des modifications qu'il a introduites. Je voudrais vous en présenter la substance avant de reprendre brièvement les quelques sujets qui me semblent appeler un commentaire.

Pour ce qui concerne la lutte contre la cybercriminalité, il est de notoriété publique que la sécurité des réseaux informatiques et de l'information a pris un poids de plus en plus déterminant sur la société et sur l'économie. Nous sommes engagés

dans une démarche pionnière qui vise à doter les États membres d'un dispositif commun afin de mieux résister aux assauts des organisations cybercriminelles et surtout de mieux collaborer. Pour ce faire, leur sont imposés un certain nombre d'exigences minimales communes, des mécanismes de prévention et de détection des incidents et de remédiation dans la mesure du possible.

Ainsi que je le disais tout à l'heure, l'exercice est limité dans la mesure où il existe déjà des exigences sectorielles au niveau européen, et car la France s'est dotée d'un dispositif normatif applicable aux organes d'importance vitale. En outre le projet de loi renvoie sur des points techniques à des dispositions réglementaires.

Concrètement, le but est d'imposer aux opérateurs dits « opérateurs de services essentiels à la société », dont la liste sera dressée par le Premier ministre, comme aux fournisseurs de services numériques – places de marché en ligne, moteurs de recherche en ligne, services d'informatique en nuage *(cloud)* – qui devront quant à eux se faire connaître auprès de l'Agence nationale de la sécurité des systèmes d'informations (ANSSI), de prendre des mesures de sécurité et de se doter ainsi, au niveau européen, d'un socle commun de protection. Les incidents, lorsqu'ils surviennent, devront être déclarés aux autorités administratives compétentes, qui pourront rendre ces informations publiques. Les opérateurs sont invités à se soumettre à des contrôles, par des organes compétents, sur pièce et sur place, à leurs frais. Enfin, un certain nombre de sanctions sont prévues.

Seront concernés, pour faire simple, les fournisseurs de services numériques et les grandes entreprises de transport, de santé, d'industrie, d'énergie, d'alimentation, etc., ainsi que les grands services publics.

Le titre II, qui rassemble les dispositions relatives au contrôle de l'acquisition et de la détention d'armes, est directement lié à la lutte contre le terrorisme et s'inscrit dans le processus d'après-2015. Le but est d'harmoniser les règles au niveau européen.

Notre système de classification et de réglementation des armes reposait, jusqu'à présent, sur une structure en quatre catégories : les armes de catégorie A, interdites ; les armes de catégorie B, soumises à autorisation ; les armes de catégorie C, soumises à déclaration ; les armes de catégorie D, réparties en deux sous-catégories, les armes dites D1 soumises à enregistrement et les D2 dont l'acquisition et la détention sont libres. Cette classification est remaniée, en procédant au surclassement d'armes de catégorie B en catégorie A : leur acquisition devient interdite, à quelques dérogations près sur lesquelles nous reviendrons. Parallèlement, du fait de cette refonte de la classification, les armes qui appartenaient à la catégorie D1, autrement dit les armes soumises à enregistrement, intègrent la catégorie C.

Enfin, la directive n'assimile plus les reproductions d'armes historiques aux armes anciennes. Elle invite à prendre en considération les techniques modernes, dès lors qu'elles recourent à des techniques modernes susceptibles d'en améliorer la durabilité et la précision, ainsi que les armes neutralisées.

Sur le fond, plusieurs dispositions sont prévues. Le contrôle administratif sur les courtiers sera renforcé et leur régime juridique aligné sur celui des armuriers ; la livraison des armes à domicile est interdite et les transactions considérées suspectes seront signalées, une fois le refus signifié.

Le titre III regroupe les dispositions relatives au service public réglementé GALILEO. Le système européen de navigation par satellite a mis du temps à se mettre en place, mais il est devenu opérationnel et actif ; il impose désormais une forme de régulation. Ce système a vocation à être équivalent aux systèmes américain GPS, russe GLONASS (глобальная навигационная спутниковая система, « système global de navigation satellitaire ») et chinois COMPASS (Beidou 北斗).

GALILEO diffuse trois catégories de signaux : un signal libre de radionavigation par satellite utilisé par les particuliers que nous sommes ; un signal commercial qu'il était prévu, au départ, de rendre payant pour les opérateurs, mais dont la gratuité sera manifestement maintenue dans les années à venir ; enfin un système robuste et sécurisé, crypté, qui exige une réglementation particulière.

Pour ce dernier système, le projet de loi met en place un mécanisme d'autorisation préalable d'accès, de fabrication de récepteurs et de réception ; il impose, tout à fait logiquement, une déclaration des transferts à l'intérieur de l'Union européenne ; est enfin prévu un dispositif de sanction au cas où les deux prescriptions ne seraient pas respectées.

J'en viens à quelques commentaires sur ce projet de loi, pour éclairer nos débats,

S'agissant de GALILEO, nous sommes dans une situation complètement contrainte qui ne pose aucune difficulté particulière : le système d'autorisation, de déclaration et de sanction se nourrit de sa propre cohérence.

Pour ce qui est de la sécurité des réseaux et des systèmes d'information, les discussions qui se sont déroulées au fil des auditions, puis en commission et en séance publique au Sénat, ont mis en lumière la nécessité d'établir une distinction entre les opérateurs de services essentiels et leurs réseaux. Il arrive qu'un même opérateur ait différents réseaux dans sa structure, qui ne nécessitent pas tous le même degré de protection.

Ainsi, lorsque la SNCF – on m'a donné cet exemple pendant les auditions – déploie un réseau numérique pour gérer ses aiguillages, on comprend qu'il s'agit de quelque chose de vital, dans la mesure où une attaque pourrait avoir pour effet de provoquer des effets mortels ; lorsqu'il s'agit de gérer la billetterie, on a affaire à un service essentiel dans la mesure où une attaque pourrait perturber considérablement la fluidité des transports dans le pays ; mais une campagne promotionnelle sur un site internet relève d'une activité tout à fait normale, qui ne nécessite pas le même degré de protection.

Pour ce qui est des armes enfin, je reviendrai sur trois points qui ne manqueront pas de faire l'objet de débats.

Une préoccupation a pu s'exprimer au sujet des armes de chasse ; je voudrais rassurer les plus inquiets. La nouvelle législation ne changera absolument rien : les armes de chasse appartenaient à la catégorie D1 et faisaient l'objet d'un enregistrement ; désormais, elles devront faire l'objet d'une déclaration. Or les règles de la déclaration sont pratiquement les mêmes que celles de l'enregistrement. Quant à l'exigence du certificat médical, elle ne tient plus dès lors qu'on est en possession d'un permis de chasse.

Pour ce qui est du transport et de la possibilité de transporter librement les armes de chasse, le code de la sécurité intérieure, dans son article R. 315-2, répond aux inquiétudes exprimées : il dispose que le permis de chasse vaut titre de transport, dès lors qu'on se trouve sur une zone de chasse et en période de chasse. Il en va de même pour les tireurs sportifs.

Les armes de collection et les armes historiques, enfin, restent d'acquisition libre. Leur reproduction, en revanche, entre désormais dans le cadre de la directive, mais seulement dans le cas où leur précision et leur durabilité ont pu être améliorées par des techniques modernes.

Certains collectionneurs ont fait part de leurs inquiétudes à l'égard de ce projet ; vous pourrez les rassurer sans délai dans vos circonscriptions, puisque l'article R. 315-3 du code de la sécurité intérieure prévoit que « *la justification de la participation à une reconstitution historique* » est un motif légitime de port et de transport d'armes. Il n'y aura donc aucun souci pour organiser une reconstitution de la bataille d'Austerlitz ou du Débarquement.

Mme la présidente Yaël Braun-Pivet. Nous en venons à la discussion générale.

M. Jean-Louis Masson. Je tiens d'abord à saluer le travail du rapporteur dans la conduite des auditions comme dans la restitution, qu'il vient de faire, d'un texte plutôt complexe au premier abord… Cela méritait d'être souligné.

Il s'agit d'adapter au droit français trois textes, dont la directive concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union. La France en est d'ailleurs l'instigatrice, car nous sommes en avance dans ce domaine sur nos partenaires européens ; sans doute est-ce dû au fait que nous disposons déjà d'une agence dédiée, l'ANSSI, qui mène très bien sa mission. Nous avons eu l'occasion d'en entendre les responsables il y a quelques jours.

Pour ce qui est du renforcement du contrôle de l'acquisition et de la détention d'armes à feu, avec la suppression de la catégorie D1 des armes à feu et le durcissement du régime d'acquisition en détention de certaines armes, nous sommes plusieurs, dont mon collègue Pierre Cordier, à nous interroger. Vous avez en partie

répondu à certaines inquiétudes ; nous y reviendrons à l'occasion des amendements, notamment à l'égard des collectionneurs.

Le transport des armes de collection sera effectivement possible dès lors que l'on participe à une reconstitution, mais il existe d'autres types de manifestations : il arrive que ces collectionneurs soient présents lors de commémorations patriotiques ; dans ce cas, le problème reste entier et plusieurs de nos amendements gardent toute leur pertinence.

Quant à la directive relative aux modalités d'accès aux services réglementés et au système mondial de radionavigation par satellite issu du programme GALILEO, elle ne nous pose *a priori* pas de difficulté particulière.

Au total, sans préjuger de ce que donnera le débat, le groupe Les Républicains est plutôt globalement favorable à ce texte, au cas des collectionneurs près, que nous aurons l'occasion d'aborder lorsque nous examinerons les amendements.

M. Jean-Michel Mis. Le projet de loi soumis à notre discussion a pour objet la transposition de deux textes européens qui concernent des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union ainsi qu'un contrôle accru de l'acquisition et de la détention d'armes. Il tire également les conséquences de la décision relative aux modalités d'accès au service public réglementé offert par le système mondial de radionavigation par satellite issu du programme GALILEO.

Ce projet de loi est une réponse à la nécessité d'harmoniser les dispositifs de sécurité avec nos voisins et partenaires européens face aux menaces d'une criminalité sans limite et sans frontières.

D'une manière générale, ce texte n'appelle pas, du fait de son objet même, beaucoup de commentaires, compte tenu de l'obligation de transposition qui est faite aux parlements nationaux et dans la mesure où nous en partageons les orientations substantielles.

Cela étant, nous devons veiller à ce que le projet de loi soumis à notre discussion ne procède pas à des surtranspositions sans motifs légitimes et justifiés, d'autant plus que cette problématique est l'une de nos priorités, comme en attestent les travaux de la mission d'information sur les moyens de lutter contre les surtranspositions des directives européennes menés par nos collègues Alice Thourot et Jean-Luc Warsmann.

Le titre I^{er} de ce projet de loi a pour but de renforcer la cybersécurité et transpose la directive européenne *Network and Information Security*, dite NIS. Cela me donne l'opportunité de saluer le travail de l'ANSSI, agence nationale de la sécurité des systèmes d'information, dont ce texte s'inspire, ainsi que la qualité du travail qui a donné lieu à la réglementation issue de la loi de programmation militaire de 2013.

Il renforce les obligations visant deux catégories de structures : les opérateurs économiques essentiels et les fournisseurs de services numériques qui, selon leur caractère plus ou moins stratégique, se verront imposer des obligations et des contrôles contraignants en matière de sécurité informatique, pouvant donner lieu à des sanctions en cas de manquement.

Ces structures devront aussi signaler aux autorités nationales compétentes en matière de cybersécurité les incidents de sécurité dont elles sont les victimes.

Le titre II introduit des dispositions relatives au contrôle de l'acquisition et de la détention d'armes qui ont pour finalité le renforcement de la sécurité publique ; elles ne concernent que l'encadrement des régimes légaux déjà existants.

Le droit applicable aux armes étant par nature principalement réglementaire, six dispositions seulement touchent à la loi.

Trois d'entre elles portent sur la classification des armes. Des armes soumises à autorisation seront dorénavant interdites ; la catégorie D1 disparaît ; les reproductions d'armes historiques ne sont plus libres d'acquisition et de détention, mais des dérogations sont prévues pour les tireurs sportifs et les personnels de la sécurité privée.

À lire certains amendements, je constate que nous avons tous été interpellés par les représentants des associations de collectionneurs qui s'inquiètent du devenir de leurs collections et de leurs prérogatives. Leurs craintes me paraissent en grande partie infondées, car les modifications opérées par la directive ne changent rien pour eux : en l'état actuel du droit, les collectionneurs ne peuvent collectionner que des armes des catégories C et D ; les armes A et B leur sont déjà interdites. Il serait malvenu, me semble-t-il, qu'à l'occasion d'une réforme visant à réduire la circulation des armes, nous autorisions l'acquisition de celles qui ne pouvaient pas l'être auparavant.

S'il est vrai qu'en 2012, le législateur avait conféré une forme de protection législative aux armes historiques et à leurs reproductions, qui restaient libres d'acquisition et de détention, la directive 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, et donc leur potentielle dangerosité. Il y va de notre sécurité à tous.

On me permettra au passage de déplorer la formulation de certains amendements reprenant des rédactions proposées par les associations de collectionneurs, où il est fait état « *d'abus d'autorité des services des douanes, de la police ou de la gendarmerie* » dans le contrôle des armes de collection. La question de la sécurité de tous doit demeurer notre priorité ; nous ne pouvons pas nous scandaliser du fait que les forces de l'ordre fassent leur travail. Mais peut-être serait-il envisageable, dans certains cas, notamment lors de reconstitutions historiques ou de commémorations patriotiques, de pouvoir mieux informer les collectionneurs de leurs droits.

Les autres dispositions, auxquelles je souscris, modifient le code de la sécurité intérieure afin de mieux encadrer la vente des armes, de leurs composants essentiels et des munitions. Pour commencer, l'ensemble des professionnels sera soumis à un contrôle portant sur leur honorabilité et leurs compétences, y compris les courtiers d'armes de catégorie C. Seront ensuite supprimées les dispositions du droit national généralisant la possibilité de livraison au domicile de l'acquéreur, en cas de vente entre particuliers, 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. Enfin, un armurier ou un courtier aura désormais la possibilité, s'il pressent une transaction suspecte, de refuser de vendre sans commettre l'infraction de refus de vente ; ils devront également signaler ces transactions aux autorités de l'État.

L'ensemble de ces dispositions me semble répondre à l'objectif de sécurité.

Le titre III, qui permet la mise en œuvre des dispositions relatives au système européen de navigation par satellite, n'appelle pas de commentaires particuliers de ma part, si ce n'est pour souligner que, grâce à ces mesures, la France pourra sortir de la dépendance des systèmes satellitaires étrangers.

Le titre IV concerne les dispositions applicables à l'outre-mer et le titre V les dispositions transitoires, et notamment la date d'entrée en vigueur de ce texte ; ils n'appellent aucun commentaire de ma part et n'ont d'ailleurs fait l'objet d'aucun amendement, si ce n'est des amendements rédactionnels.

En conclusion, ce projet de loi renforce notre sécurité et celle de nos partenaires européens ; la cybersécurité, longtemps perçue comme une affaire de spécialistes, est devenue l'affaire de tous ; le durcissement du régime pour certaines armes est une affaire de bon sens. C'est pourquoi le groupe La République en Marche lui apporte son entier soutien.

M. Jean-Luc Warsmann. Je salue d'abord, au nom du groupe UDI, Agir et Indépendants, le travail réalisé par notre rapporteur.

Je me concentrerai sur le sujet des armes. Nous avions voté et conçu de manière transpartisane ce qui est devenu la loi du 6 mars 2012. Il est toujours difficile de légiférer sur les armes. L'idée était d'être le plus sévère possible vis-à-vis de la délinquance, et le plus souple possible vis-à-vis de nos concitoyens honnêtes, chasseurs, tireurs sportifs et collectionneurs.

Or, on sent chez eux une inquiétude. Vous avez commencé à la lever, mais nous devons être très pédagogues vis-à-vis des collectionneurs. Nous sommes harcelés de sollicitations par des associations visiblement de bonne foi. L'avis du Conseil d'État apporte déjà une première réponse. Mais pouvez-vous être plus précis sur l'acquisition et la détention, et surtout sur le transport ? J'ai dans mon département une association, Ardennes 44, qui regroupe des collectionneurs d'armes américaines de la Libération ; elle se rend très régulièrement dans des manifestations pour participer à des reconstitutions, mais sans que celles-ci en soient forcément l'objet principal. Ces personnes-là sont inquiètes. Vous avez certainement matière à les rassurer, mais nous

devons être très clairs sur le sujet. Nous aurions mal travaillé si, à l'issue de nos débats, l'inquiétude subsistait à propos de ce type d'activités.

Mme Marie-France Lorho. Un projet de loi qui met en parallèle la question de l'achat d'armes et celle de la protection des données me semble bien difficile… J'avoue bien volontiers ne pas être experte en systèmes d'information et, finalement, vis-à-vis de leur sécurité, je me retrouve dans la même situation que tant de nos concitoyens : l'expectative.

Nous ne pouvons pas discuter de ce texte sans avoir en mémoire la manière dont la communauté internationale a accueilli Edward Snowden au lendemain de ses révélations sur les pratiques de la *National Security Agency* (NSA), mais aussi celles de la CIA. Aujourd'hui, nous savons qu'aucune directive européenne ne pourra rien y faire : un peu d'ingéniosité informatique suffit souvent à s'insinuer dans les systèmes les plus complexes.

Du reste, les États ne s'y sont pas trompés : ils recrutent sur des exercices de code qui visent justement à évaluer les niveaux dans ce domaine. Évidemment, il faut soutenir toutes les initiatives qui accroissent la sécurité de nos réseaux sans se faire d'illusion, et donc travailler à une société qui refuse de telles pratiques.

Encore faudrait-il pour cela donner l'exemple, et l'exemple devrait aller avec la précision de l'obligation formelle de protection des groupes gérant des données dans le domaine automobile, informatique ou téléphonique. Les articles 11, 12 et 13 vous paraissent-ils suffisamment exigeants à cet égard ?

Mme Marietta Karamanli. Je rejoins assez l'appréciation de nos collègues sur la complexité de ce texte, comme sur sa technicité.

Sur le fond, la directive « NIS » impose aux entreprises européennes d'améliorer leur capacité à résister aux cyberattaques. Pour ce faire, elle établit des normes de cybersécurité communes, elle renforce la coopération entre les différents pays de l'Union européenne ; l'objectif est bien de créer un cyber-environnement fiable au sein de l'Union européenne, en vue de soutenir le marché intérieur. C'est ce à quoi nous appelons depuis très longtemps.

Mais la directive prévoit des obligations supplémentaires, non seulement pour les États membres, mais aussi pour les particuliers responsables d'infrastructures critiques. Dans les secteurs dits essentiels, définis comme tels par chaque État, les entreprises seront tenues de prendre des mesures de sécurité adéquates afin de garantir la continuité et la sécurité de leurs réseaux et de l'information.

Elle introduit par ailleurs une obligation de notification : à compter de mai 2018, ces entreprises seront également tenues de notifier les cyber-incidents sérieux aux autorités nationales. Ce faisant, le texte institue un cadre de sécurité pour améliorer la fiabilité et la résilience des réseaux et systèmes d'information, assorti à un contrôle par l'autorité administrative, lequel peut aboutir à des sanctions.

L'article 5 définit la notion d'opérateur de services essentiels et confie au Premier ministre la responsabilité de désigner ces opérateurs. Les secteurs concernés seront l'énergie, les transports, les banques et les infrastructures ; le Gouvernement prévoit d'en ajouter d'autres comme le tourisme, l'agroalimentaire, les assurances, les affaires sociales et la construction automobile.

Cela étant, plusieurs questions se posent. La notion d'incident grave a-t-elle fait l'objet d'une définition opérationnelle, par analogie et par secteur d'activité ? Il serait intéressant de le préciser, de façon que nous puissions mieux comprendre ce domaine complexe.

S'agissant de la directive 2017/853, relative au contrôle des acquisitions et de la détention d'armes, j'ai eu précédemment l'occasion d'être rapporteure à plusieurs reprises sur cette question. Elle apporte des précisions sur les armureries et sur la vente par correspondance, mais elle ne traite que des personnes qui s'inscrivent dans un cadre légal ; elle ne s'attaque pas du tout à la problématique du trafic. C'était pourtant l'élément essentiel sur lequel nous avions insisté précédemment, à la commission des Lois comme à la commission des Affaires européennes. Que fait-on du trafic lié au reconditionnement d'armes provenant des pays des Balkans ? On les retrouve sur le marché, voire dans les mains des terroristes. Or ce texte n'aborde pas du tout ce sujet.

Enfin, le projet crée un régime d'autorisations spécifiques pour le service public réglementé offert par le service GALILEO. Développé par l'Union européenne, ce programme inclut un segment spatial dont le déploiement doit s'achever vers 2020. L'accès à ce service est limité à certains acteurs autorisés par le Gouvernement.

Ce sont à la fois la définition des secteurs concernés par le périmètre des opérateurs tenus par des obligations en matière de cybersécurité et l'ajout de dispositions sur le trafic illicite dans le cadre européen en matière de réglementation d'armes qui posent question à notre groupe. Les deux problèmes mériteraient en tout cas un débat approfondi. Peut-être nos débats d'aujourd'hui, préparatoires à la séance publique, pourront-ils apporter des compléments.

Se pose enfin la question des agences de cybersécurité. L'ANSSI dépend des services du Premier ministre. Quelle est sa position par rapport à la Commission nationale de l'informatique et des libertés (CNIL) ? L'ANSSI a 500 salariés, la CNIL n'en a que 200 ; elles interviennent par moments sur des sujets communs. Mais qu'en sera-t-il à l'avenir ? Ce point n'est pas traité.

On ne se sait pas grand-chose non plus des exigences opérationnelles formulées auprès des opérateurs, alors qu'elles sont d'une importance vitale, et entre les opérateurs à contrôler.

Sur la procédure, je formulerai seulement un regret, celui de voir ce texte, très complexe et très technique, et qui n'aborde pas tous les éléments présents dans la directive, examiné en procédure accélérée. C'est dommage. Car nous pourrions aller plus loin sur les différents sujets soulevés, comme la lutte contre le trafic ou la définition des opérateurs.

Au Sénat, peu d'amendements ont été adoptés, hormis ceux du rapporteur. Il a posé, entre autres, la question de la constitutionnalité du régime des sanctions contre les opérateurs et entreprises concernés.

Pour toutes ces raisons, le groupe Nouvelle Gauche s'abstiendra. Mais nous comptons vraiment sur ce débat et sur vos réponses, monsieur le rapporteur, pour améliorer ce texte.

M. Ugo Bernalicis. Je vais essayer de ne pas redire ce que tous les précédents collègues ont déjà dit, afin d'être efficace et d'aller à l'essentiel.

Je partage bon nombre des propos qui ont été tenus, mais, à nos yeux, ce projet de loi qui vise à transposer les règles européennes en matière de cybersécurité et d'armes arrive un peu sur le tard – peut-être est-ce pour cela d'ailleurs qu'il fait l'objet d'une procédure accélérée ?

J'ai entendu tout à l'heure que la France était plutôt à l'origine de cette directive européenne. C'est bien dommage que l'on attende le terme du délai pour la transposer, surtout en matière de cybersécurité et d'infrastructures critiques. À un moment donné, il se pose un problème de cohérence : on ne peut pas vendre le numérique à tous les coins de rue et attendre la dernière minute pour transposer les règles s'appliquant à la cybersécurité… Car nous avons attendu l'échéance du 9 mai 2018, autrement dit la date limite pour la transposition des mesures contenues dans la directive.

Pour nous, ce texte omet de traiter la question de la préservation de la souveraineté des données européennes et françaises. Pour notre groupe, les problèmes de cybersécurité des infrastructures vitales et critiques doivent s'accompagner également d'une réflexion matérielle et géographique, eu égard au caractère essentiellement filaire de l'internet européen et mondial.

Cette réponse à la question de la cybersécurité des infrastructures françaises doit passer par une approche spatialisante des infrastructures de télécom, afin que les points de fuite, via le *tapping*, soient repérés. Ainsi, certains types de données stratégiques seraient préservés de ces chemins vulnérables. Qui plus est, la multiplication des chemins de transit serait encouragée, plutôt que de laisser se former des goulets d'étranglement.

En effet, alors même que les États prétendent réduire et mieux encadrer la cybersurveillance de masse, celle-ci est toujours physiquement possible dans les infrastructures centralisées du système. Ces points de fuite propices à l'espionnage de données restent des problématiques majeures, comme en témoignent les documents révélés dans le cadre de l'affaire Snowden.

Enfin, le groupe La France insoumise regrette que le champ d'application de cette directive soit finalement réduit. Il faut au contraire élargir le champ de la loi pour que soient pris en compte tous les services essentiels. Même s'il faut contraindre tous les grands opérateurs, comme les sociétés d'autoroute, par exemple, il faut aussi

s’assurer qu’un hôpital local soit concerné par la protection des données et qu’il se conforme aux règles de sécurité vis-à-vis des cyberattaques. Mais ce dernier doit alors bénéficier d’une compensation financière sous la forme d’une aide de l’État.

On imagine mal qu’on puisse avoir, dans un certain nombre de services publics essentiels, ces cyberattaques et le vol d’un certain nombre de données sensibles. Aussi notre groupe parlementaire vous proposera-t-il un certain nombre d’amendements pour aller plus loin dans ce texte de transposition. Mais, globalement, nous en partageons l’objectif.

M. Philippe Latombe. Le texte qui nous est proposé est d’une importance insoupçonnée par beaucoup. Au-delà des articles sur les armes à feu, il contient des dispositions qui concernent les mesures permettant d’assurer un niveau élevé et commun de sécurité des réseaux et des systèmes d’information dans l’Union.

Je développerai deux points principaux.

Premièrement, la cybersécurité. Une partie du destin de la France et de l’Europe se joue dans l’espace numérique. C’est le cas pour notre économie et pour notre industrie, mais aussi pour notre sécurité collective. D’une manière générale, il s’agit d’un enjeu essentiel de souveraineté pour l’Europe.

Le second point se résume en un mot : « commun ». Je vous renvoie aux propos qu’a tenus le Président de la République dans son discours de la Sorbonne : « *Ce qui manque* le *plus à l’Europe aujourd’hui*, *c’est une culture stratégique commune*. » Les menaces désormais réelles de cybercriminalité ou de cyberattaques nécessitent une protection forte et un niveau de sécurité élevé. Pris séparément, les pays de l’Union peuvent adopter des réglementations divergentes qui pourraient laisser des failles ; l’Europe doit jouer son rôle fédérateur en ce domaine afin que la réglementation soit commune. D’où la nécessité d’un front commun sur ce sujet.

L’intérêt et l’importance de ce texte sont donc évidents : nous devons transposer le plus fidèlement possible la directive 2016/1148 du 6 juillet 2016, dite directive NIS, en adaptant notre droit interne sans surtransposer – et avant le 9 mai 2018. C’est effectivement un peu tard, mais c’est ainsi.

Le Sénat a réalisé, en procédure accélérée, un travail important et de grande qualité que je veux saluer. Le groupe MODEM et apparentés votera donc favorablement le texte présenté ; je me limiterai à trois remarques.

À l’article 6, je m’interroge sur l’opportunité de l’amendement du rapporteur. Pour l’heure, nous persistons à penser – à moins qu’il ne nous convainque du contraire – qu’il contraint plus qu’il n’autorise le décret à s’adapter aux nécessités réelles. Auquel cas il s’agirait d’une surtransposition, ce qui nous pose problème.

S’agissant de l’article 11, la rédaction adoptée par le Sénat, qui oblige tout fournisseur de service numérique offrant ses services sur le territoire national et qui n’a désigné aucun représentant dans un autre État membre de l’Union européenne à

désigner un représentant établi sur le territoire national auprès de l'autorité nationale de sécurité, nous semble de bons sens. Nous sommes très attachés à son maintien.

Plus anecdotiquement enfin, sur la détention d'armes à feu, nous souhaitons que les collectionneurs d'armes anciennes et historiques puissent continuer à s'adonner à leur passion. La rédaction adoptée par le Sénat nous laisse un peu dans l'expectative. Cela étant, les propositions d'amendements que les associations appellent de leurs vœux vont à l'encontre de la directive, ce que nous ne souhaitons pas. Une de ces revendications a été reprise dans un amendement déposé par le groupe Les Républicains ; nous souhaiterions avoir un éclairage sur ce point, afin de pouvoir rassurer tous ceux qui peuvent nous écouter.

À ces quelques points près, nous sommes en phase avec le texte et les amendements du rapporteur. Le groupe MODEM le soutiendra.

M. le rapporteur. Quelques remarques pour répondre aux principales préoccupations de nos collègues, que je comprends bien.

En ce qui concerne les collectionneurs, je rappelle que la détention des armes historiques reste inchangée : elle demeure libre. Seules passent en catégorie C les armes reproduites selon des techniques modernes pouvant en améliorer la précision et la durabilité. Quant aux armes de catégories A et B, il faut rappeler qu'elles étaient d'ores et déjà interdites aux collectionneurs : la transposition de la directive ne saurait en aucun cas ouvrir des facilités qui n'existaient pas jusqu'alors.

J'en viens à la question du caractère suffisamment strict ou non des articles 11 à 13 : j'ai pour ma part le sentiment qu'ils sont relativement « serrés ». À la demande de l'ANSSI, du Sénat et d'un certain nombre de personnes auditionnées, la précaution a été prise de mentionner les mesures devant intervenir dans chaque domaine – j'y reviendrai dans un instant.

Pour ce qui est de « l'incident significatif », permettez-moi de vous renvoyer au texte et au *1)* de l'article 6 de la directive « NIS ». Est notamment considéré comme tel un incident touchant un nombre important d'utilisateurs, qui a des conséquences sur le fonctionnement de la société, les fonctions économiques ou la sûreté publique, qui concerne un opérateur ayant des parts de marché conséquentes ou une portée géographique significative. Tous les critères sont mentionnés dans la directive et ne me paraissent pas faire l'objet de difficultés particulières.

Je comprends et partage les préoccupations relatives aux trafics d'armes, mais nous sommes là en dehors de la directive à transposer.

Il est vrai que l'on peut sans doute regretter le recours à la procédure accélérée, mais je suppose qu'elle est liée à l'étroitesse de notre marge de manœuvre : nous ne pouvons ni surtransposer ni sous-transposer et, en tout état de cause, nous devons agir dans les délais impartis.

J’en viens à la remarque, fondée, du groupe MODEM sur l’article 6. Il s’agit d’un amendement de cohérence avec ce que le Sénat a souhaité pour l’article 12. L’article 6 vise à pallier un risque d’inconstitutionnalité très légitimement soulevé au Sénat. À la suite des questionnements qui ont vu le jour en amont, et comme le Sénat l’a fait à l’article 12, je vous propose de préciser les mesures appropriées, afin de respecter le principe de légalité des délits et des peines.

Je comprends très bien les interrogations de notre collègue du groupe La France insoumise sur la protection des données personnelles. C’est essentiel dans la société dans laquelle nous vivons. Une fois encore, néanmoins, nous sommes là hors du champ de la directive, qui nous demande de transposer un nombre très réduit d’éléments.

Pour ce qui est des hôpitaux, je peux vous rassurer, ils sont mentionnés par l’annexe II de la directive au titre des opérateurs de services essentiels.

La question des acteurs d’une taille un peu moins significative est également légitime, mais il faut considérer le dispositif dans sa dynamique : dans un premier temps, un dispositif pour préserver les opérateurs d’importance vitale a été créé à l’initiative de la France, comme le corapporteur d’application l’a rappelé à juste titre ; nous sommes maintenant en train de le transposer aux opérateurs de services essentiels. Il est probable que ceux de dimension plus réduite seront ensuite appelés, dans un troisième temps, à adopter eux aussi des mesures.

Il faut prendre ce texte pour ce qu’il est : une législation pionnière, qui fait œuvre pédagogique. On peut s’émouvoir de la faiblesse des sanctions prévues, mais l’idée est de sensibiliser un certain nombre d’opérateurs à la nécessité impérieuse de se doter d’équipements de protection pour faire face aux risques de cybercriminalité.

La Commission en vient à l’examen des articles du projet de loi.

EXAMEN DES ARTICLES

TITRE I^ER
DISPOSITIONS TENDANT À TRANSPOSER 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 I^er du projet de loi se compose de quinze articles répartis en trois chapitres. Il a pour objet l'adaptation du droit français aux récentes prescriptions du droit européen en matière de cyber–sécurité. Le cadre fixé par la directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union, dite directive « *NIS* » (1), nécessite que soient prises des mesures de transposition en droit national avant le 9 mai 2018.

CHAPITRE I^ER
Dispositions communes

Article 1^er
Définitions

Résumé du dispositif et effets principaux :

Le présent article inscrit dans le droit français les définitions européennes des notions de *« réseaux et systèmes d'information »* et de *« sécurité des systèmes d'information »*.

Dispositions de la directive concernée : article 4

Modifications apportées au Sénat :

Cet article n'a fait l'objet d'aucune modification au Sénat.

Modifications apportées par votre commission des Lois :

Cet article a fait l'objet d'un amendement rédactionnel de votre rapporteur

En l'état du droit, les notions de « *réseaux et systèmes d'information* » et de « *sécurité des systèmes d'information* » ne font pas l'objet d'une définition normative générale (1). Le Conseil d'État, dans son avis sur le présent projet de

(1) Acronyme anglais de « Network and Information Security».

loi [(2)], a néanmoins estimé qu'une telle définition pourrait se révéler utile afin de mieux préciser le périmètre d'application des dispositions du titre I[er].

En conséquence, cet article reprend les définitions proposées par l'article 4 de la directive (UE) 2016/1148 précitée du 6 juillet 2016, dite directive « *NIS* », comme le montre le tableau ci–après.

Article 1[er] du projet de loi	**Article 4 de la directive « NIS »**
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 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.	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 ; 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 (…).

Cet article n'a pas fait l'objet de modification au Sénat. Une modification rédactionnelle lui a été apportée lors de son examen par votre commission.

*

* *

La Commission ***adopte*** *l'amendement de coordination rédactionnelle CL23 du rapporteur.*

---

(1) L'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les autorités administratives définit certes la notion de système d'information (« tout ensemble de moyens destinés à élaborer, traiter, stocker ou transmettre des informations faisant l'objet d'échanges par voie électronique entre autorités administratives et usagers ainsi qu'entre autorités administratives *») mais comme l'a noté le sénateur Philippe Bonnecarrère dans son rapport sur le présent projet de loi, cette définition est fortement liée à l'objet du texte et par conséquent difficilement généralisable à d'autres situations.*

(2) Conseil d'État, avis n° 393665 du 14 novembre 2017.

M. Ugo Bernalicis. Je saisis l'occasion offerte par l'examen de l'article 1er, que nous allons voter, pour revenir sur les notions de surtransposition et de sous-transposition. Je comprends bien que la sous-transposition ne soit pas possible, vu l'état actuel de notre Constitution et la hiérarchie des normes, mais je m'étonne que l'on puisse s'indigner d'une surtransposition. D'ailleurs, cela n'existe pas : il y a les textes européens, mais aussi une Assemblée nationale souveraine, qui peut voter ce qu'elle souhaite dans n'importe quel texte. Je tenais à cette mise au point. Sinon, autant dire que tous les amendements qui ont été déposés doivent être rejetés : vous nous fournirez alors un texte, on se verra cinq minutes, on votera et on repartira vers d'autres occupations… Il faut quand même garder une place pour un débat souverain dans notre pays. Avec mon groupe, je m'inscris en faux contre l'argument de la surtransposition.

M. le rapporteur. Je voudrais rassurer M. Bernalicis sur notre intention d'avoir des échanges nourris et de traiter avec la plus grande considération les amendements déposés par le groupe La France insoumise.

La Commission ***adopte*** *l'article 1er* ***modifié.***

Article 2
Champ d'application des dispositions

Résumé du dispositif et effets principaux :

Le présent article précise le champ d'application des dispositions du titre Ier du projet de loi et exclut du périmètre du projet de loi les réseaux et systèmes d'information déjà soumis, en application de normes européennes sectorielles, à des exigences en matière de sécurité des systèmes d'information, dès lors que ces exigences sont au moins équivalentes à celles crées par la nouvelle réglementation.

Dispositions de la directive concernée : 1er

Modifications apportées au Sénat :

Cet article a fait l'objet de modifications essentiellement rédactionnelles.

Modifications apportées par votre commission des Lois :

Cet article a fait l'objet de deux amendements de précision de votre rapporteur.

1. Le dispositif proposé

L'article 2 précise le champ d'application des dispositions du titre Ier du projet de loi, procédant ainsi à la transposition de l'article 1er de la directive (UE) 2016/1148 précitée du 6 juillet 2016, dite directive « *NIS* ».

Son **deuxième alinéa** dispose que les obligations prévues par le projet de loi ne seront pas applicables aux entités qui sont d'ores et déjà soumises, en application de normes européennes sectorielles, à des exigences en matière de sécurité des systèmes d'information, dès lors que ces exigences sont au moins équivalentes à celles posées par le projet de loi.

Cela concerne en particulier le secteur des communications électroniques, régi par la directive cadre 2002/21/CE du Parlement européen et du Conseil du 7 mars 2002 relative à un cadre réglementaire commun pour les réseaux et services de communications électroniques, et celui des prestataires de confiance, régi par le règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE (**alinéa premier**).

2. Les modifications apportées par le Sénat

À l'initiative de son rapporteur, la commission des Lois du Sénat a adopté un amendement remplaçant la notion d'« *entreprises exploitant des réseaux de communications électroniques ouverts au public ou fournissant des services de communications électroniques accessibles au public* » par celle d'« *opérateurs mentionnés au 15° de l'article L. 32 du code des postes et des communications électroniques* », afin d'harmoniser les définitions entre textes législatifs.

Elle a par ailleurs adopté un amendement de son rapporteur remplaçant les termes d'« *opérateurs de services essentiels* » par celui d' « *opérateurs économiques essentiels* » et simplifiant la rédaction du second alinéa sur les réseaux et systèmes d'information exclus du champ d'application de la directive. Le Gouvernement est partiellement revenu sur cette modification en séance publique – avec l'avis favorable de la Commission.

En effet, si le paragraphe 7 de l'article 1er de la directive « *NIS* » prévoit que, lorsque des dispositions sectorielles d'effet au moins équivalent à celles de la directive existent en matière de sécurité des réseaux et des systèmes d'information, celles-ci prévalent sur celles de la directive, la restriction du champ d'application de la loi appelée par cette disposition de la directive ne doit néanmoins pas conduire à exclure l'intégralité des réseaux et systèmes d'information d'entités qui répondraient à la définition d'opérateurs de services essentiels ou de fournisseurs de service numérique alors que seule une partie de ces réseaux et systèmes seraient soumis à des exigences de sécurité en vertu d'un autre acte juridique de l'Union.

Il convenait donc, afin de ne pas « sous-transposer » la directive, de rétablir l'exclusion du champ d'application du présent projet de loi pour les seuls réseaux et systèmes d'information soumis à de telles dispositions sectorielles. Ainsi les réseaux et systèmes qui sont nécessaires à la fourniture de services

essentiels ou de service numérique qui ne seront pas couverts par ces dispositions se trouveront bien dans le champ d'application du projet de loi.

3. Les modifications apportées par votre commission des Lois

À l'initiative de votre rapporteur, la Commission a adopté deux amendements de précision visant à :

– indiquer que les opérateurs de communications électroniques ne sont exemptés de ces dispositions que pour les activités d'exploitation de réseaux et de fourniture de services de communications électroniques. Ces opérateurs fournissant parfois aussi des services essentiels visés dans la catégorie « infrastructures numériques » de l'annexe II de la directive ou des services numériques de l'annexe III de la directive, ne doivent pas être exemptés au titre de ces services ;

– clarifier la portée de l'exception prévue par le second alinéa. Le deuxième alinéa de l'article 2 transpose l'article 1er, paragraphe 7, de la directive qui prévoit que, lorsque des dispositions sectorielles d'effet au moins équivalent à celles de la directive existent en matière de sécurité des réseaux et des systèmes d'information, celles-ci prévalent sur celles de la directive. La restriction du champ d'application de la loi appelée par cette disposition de la directive ne doit néanmoins pas conduire à exclure l'intégralité des réseaux et systèmes d'information d'entités qui répondraient à la définition d'opérateurs de services essentiels ou de fournisseurs de service numérique alors que seule une partie de ces réseaux et systèmes seraient soumis à des exigences de sécurité en vertu d'un autre acte juridique de l'Union. Il convenait donc, afin de ne pas sous-transposer la directive, d'exclure du champ d'application du présent projet de loi les seuls réseaux et systèmes d'information soumis à de telles dispositions sectorielles. Ainsi les réseaux et systèmes qui sont nécessaires à la fourniture de services essentiels ou de services numériques qui ne seront pas couverts par ces dispositions, se trouveront bien dans le champ d'application du projet de loi.

*

* *

La Commission ***adopte*** *successivement les amendements de précision CL29 et CL30 du rapporteur.*

Puis elle ***adopte*** *l'article 2* ***modifié.***

Article 3
Règles de confidentialité

Résumé du dispositif et effets principaux :

Le présent article précise les règles de confidentialité s'imposant à l'administration et aux prestataires de services habilités dans le cadre des activités exercées en application des dispositions du projet de loi.

Dispositions de la directive concernée : article 5

Modifications apportées au Sénat :

Le Sénat a adopté un amendement complétant les règles de confidentialité par la notion de discrétion professionnelle.

Modifications apportées par votre commission des Lois :

Cet article n'a pas fait l'objet de modification.

1. Le dispositif proposé

L'alinéa 5 de l'article 1er de la directive (UE) 2016/1148 précitée du 6 juillet 2016, dite directive « *NIS* », prévoit que chaque État membre définisse des règles afin de garantir la confidentialité des données et des informations auxquelles les services de l'État ainsi que les prestataires de service habilités à cet effet sont susceptibles d'avoir accès à l'occasion des contrôles qu'ils effectuent auprès des opérateurs économiques essentiels et des fournisseurs de service numérique.

Si le droit positif satisfait largement aux obligations de la directive s'agissant des agents publics (1), il n'existe pas de disposition similaire s'imposant aux prestataires de services privés auxquels est délégué l'accomplissement de missions de service public.

Le **premier alinéa du présent article** prévoit donc, à cet effet, que les prestataires de services habilités à effectuer des contrôles dans le cadre des dispositions du texte respectent les mêmes règles de confidentialité que celles qui s'imposent aux services de l'État.

Il dispose par ailleurs que le Premier ministre peut – dans les conditions définies aux articles 7 et 13 du projet de loi – informer le public ou un autre État

(1) Ainsi, l'article 26 de la loi n° 83-634 du 11 juillet 1983 portant droits et obligations des fonctionnaires dispose que les agents publics sont tenus au secret professionnel et soumis à une obligation de discrétion professionnelle « pour tous les faits, informations ou documents dont ils ont connaissance dans l'exercice ou à l'occasion de l'exercice de leurs fonctions ». De surcroît, l'article L. 311-6 du code des relations entre le public et l'administration dispose que ne sont communicables qu'à la personne, physique ou morale, intéressée, les documents administratifs qui porteraient atteinte aux informations économiques et financières et aux stratégies commerciales et industrielles.

membre d'un incident affectant le système d'information d'un opérateur économique essentiel ou d'un fournisseur de service numérique.

Comme l'impose l'article 14 de la directive « *NIS* », le **second alinéa** prévoit que l'État veille, lorsqu'il procède à une telle information, aux intérêts économiques de ces entités et à ne pas révéler d'informations susceptibles de porter atteinte à leur sécurité et au respect en matière industrielle et commerciale. Cette précision ne s'applique qu'à « *l'autorité administrative compétente* », les prestataires de service habilités n'étant pas autorisés à communiquer sur un incident. Cette mission incombera à l'Agence nationale de la sécurité des systèmes d'information (ANSSI). Cette agence, créée par le décret n° 2009-834 du 7 juillet 2009, est un service à compétence nationale rattaché au Secrétaire général de la défense et de la sécurité nationale, chargée de :

– détecter et réagir au plus tôt en cas d'attaque informatique, grâce à un centre de détection chargé de la surveillance permanente des réseaux sensibles et de la mise en œuvre de mécanismes de défense adaptés aux attaques ;

– prévenir la menace par le développement d'une offre de produits de très haute sécurité ainsi que de produits et services de confiance pour les administrations et les acteurs économiques ;

– jouer un rôle de conseil et de soutien aux administrations et aux opérateurs d'importance vitale ;

– informer régulièrement le public sur les menaces.

2. Les modifications apportées par le Sénat

De manière à clarifier le champ de l'obligation définie au premier alinéa, la commission des Lois du Sénat a adopté un amendement de son rapporteur complétant les règles de confidentialité par la notion de discrétion professionnelle et précisant que les règles visées sont celles s'imposant aux services de l'État ainsi qu'aux agents publics. Elle a par ailleurs substitué au terme « *État* » l'expression d'*« autorité administrative compétente* », qui vise plus directement l'ANSSI.

*

* *

La Commission ***adopte*** *l'article 3* ***sans modification.***

Article 4
Application réglementaire

Résumé du dispositif et effets principaux :

Le présent article prévoit que les modalités d'application du titre I[er] du projet de loi – en particulier la liste des services essentiels au fonctionnement de la société ou de l'économie – sont déterminées par décret en Conseil d'État.

Modifications apportées au Sénat :

Le Sénat a complété le champ d'application du décret qui devra préciser, pour chacun des domaines mentionnés à l'article 12 du présent projet de loi, la nature des mesures de sécurité qui devront être mises en oeuvre par les fournisseurs de service numérique.

Modifications apportées par votre commission des Lois :

Cet article n'a pas fait l'objet de modification.

Le présent article prévoit que les modalités d'application du titre I[er] du projet de loi seront déterminées par décret en Conseil d'État. Il précise que ce décret fixera notamment la liste des services essentiels au fonctionnement de la société ou de l'économie mentionnés à l'article 5 du projet de loi.

Par un amendement de son rapporteur, la commission des Lois du Sénat a complété cet article afin d'indiquer que le décret précisera également, pour chacun des domaines mentionnés à l'article 12, la nature des mesures de sécurité qui devront être mises en œuvre par les fournisseurs de service numérique [(1)].

*

* *

*La Commission **adopte** l'article 4 **sans modification**.*

(1) Cf. commentaire de l'article 12.

CHAPITRE II
Dispositions relatives à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels

Article 5
Définition des opérateurs de services essentiels

Résumé du dispositif et effets principaux :

Le présent article précise la notion d'opérateurs de services essentiels et fixe les modalités de leur désignation.

Dispositions de la directive concernée : article 5

Modifications apportées au Sénat :

Le Sénat a adopté des amendements substituant à la notion de « *perturbation grave* » affectant les opérateurs de services essentiels celle de *« rupture de continuité de service* » et précisant que ne sont exclus du champ d'application de la présente loi que les systèmes d'information des opérateurs d'importance vitale et non les opérateurs eux-mêmes.

Modifications apportées par votre commission des Lois :

Cet article a fait l'objet d'un amendement de précision de votre rapporteur.

1. Le dispositif proposé

Le **premier alinéa du présent article** détermine les critères permettant de définir un opérateur de services essentiels (OSE). Il s'agit de ceux édictés par l'article 5 de la directive (UE) 2016/1148 précitée du 6 juillet 2016, dite directive « *NIS* » :

– l'**activité** inclut la fourniture de services essentiels au fonctionnement de la société et de l'économie. Cette définition est plus large que celle utilisée par la directive, qui n'inclut que les services essentiels « *au maintien d'activités sociétales et/ou économiques critiques* ». En effet, si la directive identifie sept secteurs répondant à la notion de services économiques essentiels (l'énergie, les transports, les banques, les infrastructures et marchés financiers, la santé, la fourniture et la distribution d'eau potable et les infrastructures numériques), l'étude d'impact associée au présent projet de loi indique toutefois que cette liste pourrait s'élargir à d'autres secteurs ;

– la fourniture de services essentiels doit reposer sur **l'utilisation de réseaux et systèmes d'information** ;

– tout incident affectant ces réseaux et systèmes d'information doit être **susceptible d'entraîner une perturbation grave des services essentiels** qu'il

fournit. À cet égard, le 1 de l'article 6 de la directive « *NIS* » fournit une liste de critères – non exhaustive – permettant aux États membres de déterminer l'importance d'un effet disruptif :

– le nombre d'utilisateurs tributaires du service concerné ;

– la dépendance d'autres secteurs considérés comme essentiels à l'égard du service affecté par un incident ;

– les conséquences que des incidents pourraient avoir, en termes de degré et de durée, sur les fonctions économiques, sociétales ou sur la sûreté publique ;

– la part de marché de l'opérateur concerné ;

– la portée géographique de l'incident ;

– l'importance que revêt l'opérateur pour garantir un niveau suffisant de service dans le secteur ou le sous-secteur concerné, compte–tenu de la disponibilité de solutions de rechange pour la fourniture de ce service.

Le 2 de l'article 6 de la directive « *NIS* » permet en outre aux États membres de tenir compte de critères sectoriels.

Les opérateurs de services essentiels seront nominativement désignés par un arrêté du Premier ministre, sur la base des critères précédemment exposés. La liste devrait faire l'objet d'une mise à jour régulière, au minimum tous les deux ans, comme le prévoit l'alinéa 5 de l'article 5 de la directive « *NIS* ».

Le **second alinéa** du présent article exclut du périmètre des OSE les systèmes d'information des opérateurs d'importance vitale (OIV), définis comme les « *opérateurs publics ou privés exploitant des établissements ou utilisant des installations et ouvrages, dont l'indisponibilité risquerait de diminuer d'une façon importante le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la nation* » (1) .

Comme le souligne l'étude d'impact associée au présent projet de loi, cette exclusion parait logique dès lors que « *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*

(1) Article L. 1332-1 du code de la défense.

importante le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la nation » 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.

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. »

Par ailleurs, il faut noter que certaines entreprises sont susceptibles de répondre à la fois à la définition d'OIV et à celle d'OSE en fonction des systèmes d'information concernés. Ainsi, pour reprendre l'exemple donné par l'ANSSI lors de son audition par votre rapporteur, la SNCF dispose d'au moins trois systèmes d'information dont la sensibilité est très variable :

– le système d'aiguillage, d'importance vitale puisqu'un important dysfonctionnement serait susceptible de mettre en danger des vies humaines ;

– le système de billetterie, service essentiel puisqu'un dysfonctionnement conséquent répond aux critères énoncés par la directive « *NIS* » ;

– le site d'information générale et de promotion de la SNCF, qui ne revêt pas un caractère stratégique.

Ces différences de sensibilité expliquent la nécessité de conserver des régimes distincts car les OIV, dont le nombre s'élève à 230, sont soumis à des règles particulièrement strictes en matière de sécurité des systèmes d'information, qui ne paraissent pas nécessairement justifiées pour l'ensemble des systèmes et réseaux d'information des entreprises.

2. Les modifications apportées par le Sénat

La commission des Lois du Sénat a adopté deux amendements de son rapporteur visant à substituer à la notion de « *perturbation grave* » affectant les OSE celle de « *rupture de continuité de service* » et à apporter au dispositif proposé quelques modifications rédactionnelles.

Lors de la séance publique, le Sénat a adopté, à l'initiative du Gouvernement et avec l'avis favorable de la Commission, un amendement précisant que ne sont exclus du champ d'application de la présente loi que les systèmes d'information visés à l'article L. 1332-6-1 du code de la défense et non les OIV eux-mêmes. En effet, comme cela a été démontré plus haut, un même opérateur doit pouvoir se voir appliquer le dispositif visé par la directive « *NIS* » pour certains de ses systèmes d'information nécessaires à la fourniture de services essentiels et le dispositif applicable aux opérateurs d'importance vitale pour d'autres de ses systèmes.

3. Les modifications apportées par votre commission des Lois

À l'initiative de votre rapporteur, la commission a adopté un amendement de clarification. Les opérateurs d'importance vitale, mentionnés aux articles L. 1332-1 et L. 1332-2 du code de la défense voient certains de leurs systèmes d'information soumis, en application des articles L. 1332-6-1 et suivants du code de la défense à des exigences plus strictes que celles prévues par la directive.

Certains de ces opérateurs ont par ailleurs vocation à être désignés comme opérateurs de services essentiels compte tenu de la liste des types d'entités figurant à l'annexe II de la directive. En première approche, ceux-ci pourraient donc être exclus du champ d'application du présent projet de loi puisqu'ils sont déjà soumis à des obligations au moins équivalentes, ainsi que le permet l'article 3 de la directive.

Toutefois, 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 et à ce titre ne concerne que les systèmes d'information de ces opérateurs en lien avec la sécurité nationale (ces systèmes sont définis à l'article L. 1332-6-1 du code de la défense).

La directive s'inscrit, elle, dans le cadre du fonctionnement des activités économiques et sociétales du marché intérieur européen et, en conséquence, s'applique à des systèmes d'information en lien avec de telles activités.

Afin que la transposition de la directive soit complète, un même opérateur doit donc pouvoir se voir appliquer le dispositif visé par la directive pour certains de ses systèmes nécessaires à la fourniture de services essentiels et le dispositif applicable aux opérateurs d'importance vitale pour d'autres de ses systèmes.

Il convenait donc de n'exclure du champ d'application de la présente loi que les systèmes d'information visés à l'article L. 1332-6-1 du code de la défense et non les opérateurs d'importance vitale eux-mêmes.

*

* *

La Commission examine l'amendement CL20 de M. Ugo Bernalicis.

M. Ugo Bernalicis. Cet amendement, que j'ai déjà un peu dévoilé tout à l'heure, vise à renforcer la lutte contre les cyberattaques en protégeant spécifiquement un certain nombre de services à nos yeux fondamentaux – et je suis sûr que vous partagerez ce constat.

Imaginez, au cours d'une opération à cœur ouvert, que les ordinateurs ne fonctionnent plus et provoquent un dysfonctionnement d'un appareil permettant de maintenir le rythme cardiaque. Ce serait pour le moins regrettable…

Imaginez qu'une agence de Pôle emploi soit piratée et que l'intégralité de sa base de données soit effacée ou, plus insidieusement, partiellement modifiée, ce qui ne permettrait plus aux ayants droit de bénéficier de leur dû.

Imaginez enfin que nos logiciels Eliasse ou Eloi soient piratés et que tous les amendements déposés par le groupe La France insoumise passent sous la signature de députés de La République en Marche et que vous les votiez par inadvertance !

Plus sérieusement, nous considérons qu'il faut davantage protéger un certain nombre de services essentiels dans les domaines social, éducatif, économique, environnemental, sanitaire, médico-sociaux et culturels. Il nous semble donc nécessaire d'aller au-delà du projet de loi : l'amendement propose d'inclure explicitement ces domaines fondamentaux pour le bien-être collectif, dans le strict respect de la répartition des compétences entre l'exécutif et le législatif.

M. le rapporteur. On a le poil qui se hérisse d'effroi avec certains de vos exemples. *(Sourires.)*

Je reviens sur une réponse que je vous ai déjà faite, et qui montre que nous traitons vos amendements avec la plus grande considération : les hôpitaux entrent d'ores et déjà dans le cadre prévu par la directive. Dans son annexe II, tous les secteurs concernés sont mentionnés, l'énergie, les transports, les banques, les infrastructures de marchés financiers, le secteur de la santé, avec les hôpitaux et les cliniques, mais aussi l'eau potable et les infrastructures numériques. Par ailleurs, le Gouvernement s'est engagé à élargir ultérieurement le champ d'application du texte. Par conséquent, j'émets un avis défavorable.

M. Ugo Bernalicis. Notre liste a le mérite de l'exhaustivité et de figurer non pas dans une annexe, mais directement dans le projet de loi. Elle nous semble plus précise et plus englobante. Si les hôpitaux sont mentionnés par la directive, très bien, mais je ne crois pas que Pôle emploi entre dans un des domaines que vous avez cités, à moins de leur donner des définitions extrêmement larges et de considérer que tout est dans l'annexe – mais je ne crois pas que ce soit le cas. Par conséquent, je maintiens mon amendement, en espérant un vote favorable.

*La Commission **rejette** l'amendement.*

*Puis elle **adopte** l'amendement de clarification CL31 du rapporteur.*

*La Commission **adopte** ensuite l'article 5 **modifié**.*

Article 6
Règles minimales en matière de protection des réseaux et système d'information

Résumé du dispositif et effets principaux :

Le présent article détermine le régime d'obligations applicable aux opérateurs de services essentiels en matière de sécurité des réseaux et systèmes d'information.

Dispositions de la directive concernée : article 14

Modifications apportées au Sénat :

Le Sénat a adopté cet article sans modification.

Modifications apportées par votre commission des Lois :

Cet article a fait l'objet d'un amendement de précision de votre rapporteur.

Le **premier alinéa du présent article** prévoit que le Premier ministre fixe les règles de sécurité nécessaires à la protection des réseaux et des systèmes d'information des opérateurs de services essentiels (OSE). Ce faisant, il transpose en droit français le 2 de l'article 14 de la de la directive (UE) 2016/1148 précitée du 6 juillet 2016, dite directive « *NIS* », aux termes duquel il est prévu que « [l]*es 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*. » Le premier alinéa précise en outre que les OSE appliqueront ces règles à leurs frais.

Le **deuxième alinéa du présent article** prévoit que les règles prévues à l'alinéa précédent peuvent comprendre la prescription du recours à certains dispositifs matériels ou logistiques.

Le Sénat a adopté cet article sans modification. Votre Commission a complété cet article en détaillant les catégories de mesures qui devront être mises en œuvre par les opérateurs, étant entendu que celles-ci seront précisées de manière réglementaire compte tenu de la technicité du sujet.

*

* *

*La Commission **adopte** l'amendement de précision CL35 du rapporteur.*

*Puis elle **adopte** l'article 6 **modifié**.*

Après l'article 6

La Commission est saisie de l'amendement CL19 de Mme Danièle Obono.

Mme Danièle Obono. L'amendement demande la production d'un rapport évaluant les coûts supplémentaires pour les opérateurs privés à but non lucratif, en particulier les organisations non gouvernementales (ONG) considérées comme des opérateurs au sens de l'article 5. Il s'agit de combler une lacune de l'étude d'impact, qui n'évalue pas précisément le coût pour les acteurs entrant dans le champ établi par le Premier ministre, quel que soit leur statut.

Ce faisant, nous relayons les inquiétudes légitimes d'ONG qui pourraient être qualifiées d'opérateurs de services essentiels, comme les Restaurants du Cœur, dans la mesure où ils fournissent des repas à beaucoup d'hommes et de femmes démunis, ou des associations auxquelles est confiée la gestion du service public de l'accueil des demandeurs et demandeuses d'asile. Ces exemples nous obligent à nous interroger sur l'impact budgétaire de ce texte, alors que l'équilibre financier de telles structures est déjà très fragile. Notre amendement permettra de répondre à des questions sensibles.

M. le rapporteur. Avis défavorable. Le coût sera précisé dans la fiche d'impact qui accompagnera les textes réglementaires d'application, mais il existe déjà des fourchettes permettant de savoir où l'on va : pour les opérateurs d'importance vitale, les montants sont compris entre un et deux millions d'euros jusqu'à présent. On sera donc en deçà, puisque le degré d'exigence sera moindre. Il faut aussi prendre en compte la logique globale : il s'agit de se préserver des coûts colossaux qui peuvent être causés par la cybercriminalité – 250 millions d'euros pour Saint-Gobain, par exemple. La culture est en train de changer chez les opérateurs : ils s'aperçoivent que les coûts sont dérisoires par rapport à ceux des attaques.

Mme Danièle Obono. Nous sommes d'accord, mais l'amendement CL19 concerne des ONG. Dans la perspective d'une compensation financière pour ces acteurs, via une aide de l'État, il faudrait que le Parlement sache précisément où l'on en est. Ces structures n'ont souvent pas les moyens financiers de se protéger. C'est tout l'intérêt de ce rapport.

*La Commission **rejette** l'amendement.*

Article 7
Obligation de signalement des incidents

Résumé du dispositif et effets principaux :

Le présent article introduit, à l'égard des opérateurs de services essentiels, une obligation de signalement à l'agence nationale de sécurité des systèmes d'information (ANSSI) de certains incidents et fixe les conditions dans lesquelles l'administration est autorisée à communiquer sur un tel incident.

Dispositions de la directive concernée : article 14

Modifications apportées au Sénat :

Le Sénat a adopté deux amendements, précisant, d'une part, que l'obligation de signalement ne serait opposable aux entreprises qu'à compter de la découverte de l'incident et, laissant, d'autre part, une marge de manœuvre plus grande au pouvoir réglementaire s'agissant du choix de l'autorité compétente pour procéder à l'information du public.

Modifications apportées par votre commission des Lois :

Cet article n'a fait l'objet d'aucune modification.

1. Le dispositif proposé

Le **I du présent article** crée une obligation de signalement par les opérateurs de services essentiels (OSE) de certains incidents, transposant ainsi les 3 et 4 de l'article 14 de la directive (UE) 2016/1148 précitée du 6 juillet 2016, dite directive « *NIS* ».

Les OSE seront tenus de signaler à l'ANSSI, sans retard injustifié, tous les incidents qui ont un impact significatif sur la continuité des services essentiels qu'ils fournissent. Comme prévu à l'article 14 de la directive « *NIS* », l'impact significatif se caractérise par le nombre d'utilisateurs et la zone géographique touchés, ainsi que par la durée de l'incident.

S'inscrivant dans une démarche de prévention et de pédagogie, cet alinéa impose également aux OSE une obligation de signalement des incidents dont l'impact serait « *susceptible* » d'être significatif, ce qui n'est pas prévu par la directive « *NIS* ».

L'attention de votre rapporteur a été appelée lors de ses auditions sur les difficultés engendrées par la multiplication récente des obligations de signalement imposées aux entreprises. Il se joint aux observations du sénateur Bonnecarrère sur le présent projet de loi qui a souligné dans son rapport que « *les entreprises éprouv[ent] de plus en plus de difficultés à concilier des obligations de signalement d'incidents de sécurité de nature similaire, imposés par différents*

textes juridiques (le règlement général de protection des données personnelles, la réglementation sur les opérateurs de communications électroniques, le règlement européen ePrivacy, etc.). Ainsi, dans le cas d'un incident affectant un traitement de données à caractère personnel dans le domaine de la santé, une entreprise est contrainte d'effectuer une déclaration auprès de l'ANSSI, de la Commission nationale de l'informatique et des libertés (CNIL) et de l'agence régionale de santé. Bien que la rationalisation de ces dispositifs dépasse le cadre du projet de loi, [il]estime qu'il pourrait être nécessaire de conduire une réflexion afin de simplifier, pour les entreprises, ces procédures de signalement. » (1)

Le **II du présent article** détermine par ailleurs, comme le prévoit l'alinéa 6 de l'article 14 de la directive « *NIS* », les conditions dans lesquelles il peut être procédé à une information ou une sensibilisation du public en cas de survenance d'un incident. En raison de la confidentialité potentielle des informations concernées, l'opérateur serait préalablement informé. Par ailleurs, comme prévu par l'alinéa 5 du même article 14, dans les cas où un incident aurait un impact transfrontalier, le Premier ministre serait tenu d'en informer les autorités compétentes des États membres concernés.

2. Les modifications apportées par le Sénat

La commission des Lois du Sénat a adopté, à l'initiative de son rapporteur, un amendement permettant de mieux encadrer les délais de signalement à l'ANSSI, compte–tenu du fait que la détection d'intrusions informatiques dans un système d'information pouvait prendre du temps. Il lui est donc apparu pertinent de s'éloigner de la notion de « *retard injustifié* » présente à l'alinéa 3 de l'article 14 de la directive « *NIS* » afin de préciser que l'obligation de signalement ne serait opposable aux entreprises qu'à compter de la découverte de l'incident, comme cela est notamment le cas à l'article 33 du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (RGPD), s'agissant de la notification à l'autorité de contrôle d'une violation de données à caractère personnel (2).

S'agissant de l'information du public, la commission des Lois du Sénat a substitué, à l'initiative de son rapporteur, aux termes de « *Premier ministre* » les termes d'« *autorité administrative* », laissant ainsi une marge de manœuvre au pouvoir réglementaire pour préciser les autorités compétentes ainsi que les délégations qui pourront, le cas échéant, être mises en place.

---

(1) Sénat, rapport n° 161 de M. Philippe Bonnecarrère sur le projet de loi portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité, 13 décembre 2017.

(2) Premier alinéa de l'article 33 du RGPD : « En cas de violation de données à caractère personnel, le responsable du traitement en notifie la violation en question à l'autorité de contrôle compétente conformément à l'article 55, dans les meilleurs délais et, si possible, 72 heures au plus tard après en avoir pris connaissance, à moins que la violation en question ne soit pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques. Lorsque la notification à l'autorité de contrôle n'a pas lieu dans les 72 heures, elle est accompagnée des motifs du retard ».

*

* *

La Commission examine l'amendement CL18 de M. Ugo Bernalicis.

M. Ugo Bernalicis. L'amendement CL18 tend à instaurer une obligation d'informer le Parlement en cas d'incidents affectant les réseaux et les systèmes d'information nécessaires à la fourniture des services essentiels et ayant un impact significatif sur la continuité de ces derniers. Pour notre groupe, il est fondamental que le Parlement puisse être informé de l'état de la menace « cyber » en France, dans un cadre respectueux de l'équilibre des pouvoirs. Nous proposons une obligation d'information, avec l'encadrement de l'ANSSI pour assurer la confidentialité des données, afin de permettre aux commissions parlementaires compétentes d'être réactives face aux différents types de menaces et à leur évolution, en lien avec le Gouvernement.

M. le rapporteur. Je vous rejoins pour ce qui concerne l'information des parlementaires : nous sommes également sensibles au fait qu'une démocratie vivante suppose un Parlement actif, tenu au courant des difficultés qu'un certain nombre de secteurs peuvent rencontrer. En revanche, une information systématique, à chaque attaque de cybercriminalité, me paraît complètement disproportionnée, d'autant que nous avons la faculté d'auditionner l'ANSSI autant que de besoin. En cas de récurrence évidente d'incidents, nous ne manquerions pas de le faire, madame la présidente.

M. Ugo Bernalicis. Nous n'avions pas la prétention de demander que 100 % des cyberattaques nous soient signalées : nous visons les cyberattaques affectant un service essentiel et ayant un impact significatif sur sa continuité. Ces éléments seraient probablement de notoriété publique, mais il ne vous a pas échappé qu'une attaque sur les données d'un « transporteur » ayant recours à des véhicules de tourisme, si je puis dire, car je ne voudrais pas citer de nom, a mis du temps à être connue du grand public, ce qui peut poser un problème. Les données personnelles ne sont pas une marchandise comme les autres. Il nous semble important que le Parlement soit informé des faits les plus significatifs. On peut auditionner l'ANSSI, et c'est tant mieux, mais ce que nous vous proposons est un peu différent.

La Commission ***rejette*** *l'amendement.*

L'article 7 est ***adopté sans modification.***

Article 8
Modalités de contrôle

Résumé du dispositif et effets principaux :

Le présent article prévoit la possibilité pour l'autorité administrative d'effectuer ou de faire pratiquer des contrôles auprès des opérateurs de services essentiels (OSE) ainsi que la mise en place d'un pouvoir d'injonction à l'encontre des OSE.

Dispositions de la directive concernée : article 15

Modifications apportées au Sénat :

Le Sénat a précisé le dispositif d'injonction prévu afin d'instituer un délai adapté en fonction des circonstances à l'OSE pour se mettre en conformité avec ses obligations.

Modifications apportées par votre commission des Lois :

Cet article a fait l'objet d'un amendement rédactionnel de votre rapporteur.

1. Le dispositif proposé

Le **premier alinéa du présent article** prévoit, afin d'assurer l'effectivité du dispositif de cybersécurité mis en place par le projet de loi, que le Premier ministre peut soumettre les OSE à un certain nombre de contrôles. Ce faisant, il transpose le 1 de l'article 15 de la directive (UE) 2016/1148 précitée du 6 juillet 2016, dite directive « *NIS* ».

Aux termes du **deuxième alinéa du présent article**, les contrôles sont effectués sur pièce et sur place, par l'Agence nationale de sécurité des systèmes d'information (ANSSI) ou par des prestataires de services qualifiés et habilités par le Premier ministre. Le coût des contrôles est à la charge de l'OSE. Le rapport précité du sénateur Philippe Bonnecarrère précise que « *le coût estimé pourrait s'élever à 1 200 euros/jour/homme. Cette charge, bien que non négligeable pour les entreprises, ne paraît pas (…) disproportionnée au regard, d'une part, de la capacité des opérateurs économiques essentiels à l'absorber, d'autre part du fait que les contrôles menés auprès d'un même opérateur devraient être assez espacés dans le temps.* » [(1)]

Le **troisième alinéa** institue – comme prévu au 2 de l'article 15 de la directive « *NIS* » – une obligation de transmission, à l'autorité ou au prestataire responsable du contrôle, de toutes les informations nécessaires pour le réaliser. Cela est susceptible d'inclure les documents relatifs à la politique de sécurité ainsi que les résultats d'audits de sécurité. En outre, logiquement, il est prévu que l'ANSSI ou le prestataire chargé du contrôle seront autorisés à accéder aux

(1) Sénat, rapport n° 161 de M. Philippe Bonnecarrère, op. cit.

réseaux et systèmes d'information de l'OSE concerné afin d'effectuer des analyses et des relevés d'informations techniques.

Le **quatrième alinéa** dispose que les OSE corrigent tout manquement à leurs obligations qui aurait été constaté dans le délai imparti par la mise en demeure notifiée à l'issue du contrôle, ce qui correspond à la transposition des « *instructions contraignantes* » prévues par le 3 de l'article 15 de la directive « *NIS* ».

2. Les modifications apportées par le Sénat

À l'initiative de son rapporteur, la commission des Lois du Sénat a réécrit le dispositif d'injonction afin de préciser que le délai fixé devra tenir compte des conditions de fonctionnement de l'OSE et des mesures à mettre en œuvre. Elle a par ailleurs procédé à plusieurs modifications d'ordre rédactionnel.

*

* *

*La Commission **adopte** l'amendement rédactionnel CL32 du rapporteur.*

*Puis elle **adopte** l'article 8 **modifié.***

Article 9
Sanctions pénales

Résumé du dispositif et effets principaux :

Le présent article détermine les sanctions pénales encourues par les opérateurs de services essentiels en cas de manquement aux obligations fixées par le projet de loi.

Dispositions de la directive concernée : article 21

Modifications apportées au Sénat :

Le Sénat a adopté un amendement de coordination avec les modifications apportées à l'article 8.

Modifications apportées par votre commission des Lois :

Cet article a fait l'objet d'un amendement rédactionnel de votre rapporteur.

1. Le dispositif proposé

L'article 21 de la de la directive (UE) 2016/1148 précitée du 6 juillet 2016, dite directive « *NIS* », prévoit que 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. »

En conséquence, le présent article crée trois nouvelles infractions :

– celle, prévue au **premier alinéa**, qui sanctionne le fait de ne pas se conformer aux règles de sécurité imposées aux opérateurs de services essentiels (OSE) nécessaires à la protection des réseaux et systèmes d'information [(1)]. Elle est sanctionnée d'une amende de 100 000 euros ;

– celle, prévue au **deuxième alinéa**, qui pénalise le fait de ne pas satisfaire à l'obligation de déclaration d'incidents à l'ANSSI [(2)]. Elle est passible d'une amende de 75 000 euros ;

– celle, prévue au **troisième alinéa**, qui punit d'une amende de 125 000 euros le fait de faire obstacle aux opérations de contrôle des obligations de sécurité [(3)].

La responsabilité pénale incomberait aux dirigeants des opérateurs concernés.

Ces montants paraissent à la fois effectifs, proportionnés et dissuasifs comparés à ceux prévus pour d'autres infractions dans le domaine de la cybersécurité, comme l'illustre le tableau ci–dessous.

Type d'opérateurs ou de données concernées	**Sanctions**
Opérateurs d'importance vitale	Article L. 1332–7 du code de la défense Est puni d'une amende de 150 000 euros le fait, pour les dirigeants des opérateurs mentionnés à l'article L. 1332-4 et à l'expiration du délai défini par l'arrêté de mise en demeure, d'omettre d'établir un plan de protection ou de réaliser les travaux prévus. Est puni d'une amende de 150 000 euros le fait, pour les mêmes personnes, d'omettre, après une mise en demeure, d'entretenir en bon état les dispositifs de protection antérieurement établis. Est puni d'une amende de 150 000 € le fait, pour les mêmes personnes, de ne pas satisfaire aux obligations prévues aux articles L. 1332-6-1 à L. 1332-6-4. Hormis le cas d'un manquement à l'article L. 1332-6-2, cette sanction est précédée d'une mise en demeure.
Traitement de données personnelles	Article 226–17 du code pénal Le fait de procéder ou de faire procéder à un traitement de données à caractère personnel sans mettre en œuvre les mesures prescrites à l'article 34 de la loi n° 78-17 du 6 janvier 1978 précitée est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende.

(1) Cf. commentaire de l'article 6 du projet de loi.

(2) Cf. commentaire de l'article 7 du projet de loi.

(3) Cf. commentaire de l'article 8 du projet de loi.

À l'initiative de son rapporteur, la commission des Lois du Sénat a adopté un amendement d'amélioration rédactionnelle, par coordination avec les modifications qu'elle a apportées à l'article 8.

*

* *

La Commission examine, en discussion commune, les amendements CL25 du rapporteur, CL17 de Mme Danièle Obono et CL15 de M. Ugo Bernalicis.

M. le rapporteur. Mon amendement CL25 est rédactionnel.

Mme Danièle Obono. Afin d'assurer la sécurité des réseaux et des systèmes d'information, l'amendement CL15 vise à augmenter le montant de l'amende susceptible d'être prononcée. Il s'agit de la rendre plus efficace et réellement dissuasive. Compte tenu de leur poids économique, des opérateurs numériques tels que Google, Apple, Facebook ou Amazon, les GAFA, peuvent facilement « absorber » des montants aussi dérisoires que ceux proposés dans le texte. La législation risquerait donc d'être inutile à leur égard, tandis qu'elle pèserait plus lourdement sur les petites et moyennes entreprises. Quant à l'amendement CL17, il vise à élargir le champ des personnes morales susceptibles d'être frappées d'une amende.

M. le rapporteur. On peut comprendre les préoccupations liées à la faiblesse des amendes, mais ce sujet doit être abordé sous un double prisme. Ce texte, pionnier, a d'abord une vocation pédagogique : il incite les entreprises à adopter un seuil minimal de protection. Ensuite, nous sommes dans la transposition d'une directive et il existe déjà des sanctions pénales qui peuvent s'appliquer aux opérateurs d'importance vitale : celles pour les opérateurs de services essentiels ont été fixées en conséquence, car on ne peut pas imaginer une disproportion par rapport à l'étage supérieur. Avis défavorable.

M. Ugo Bernalicis. Nous proposons de porter les sanctions jusqu'à 4 % du chiffre d'affaires, mais cela ne veut pas dire qu'elles atteindront systématiquement un tel niveau. Il faut pouvoir proportionner la réponse. On peut entendre l'argument touchant à la pédagogie quand il s'agit des petites entreprises, mais je pense que les grands groupes sont à peu près au courant de la cybercriminalité, puisqu'ils subissent régulièrement des cyberattaques. Je le répète : les données personnelles ne sont pas des données comme les autres. Elles font partie de notre identité individuelle. Nous sommes tous sur les réseaux sociaux, nous avons tous un smartphone et des comptes chez Google ou d'autres. Ce n'est donc pas une mince affaire. Il est déterminant de s'assurer que la sanction sera conséquente en cas de manquement, notamment vis-à-vis des GAFA.

*La Commission **adopte** l'amendement CL25. En conséquence, les amendements CL17 et CL15 tombent.*

*La Commission **adopte** ensuite l'article 9 **modifié**.*

CHAPITRE III
Dispositions relatives à la sécurité des réseaux et des systèmes d'information des fournisseurs de service numérique

Article 10
Définition des fournisseurs de service numérique

Résumé du dispositif et effets principaux :

Le présent article définit les notions de service numérique et de fournisseur de service numérique.

Dispositions de la directive concernée : article 4

Modifications apportées au Sénat :

Le Sénat a adopté un amendement corrigeant une erreur de référence.

Modifications apportées par votre commission des Lois :

Cet article n'a fait l'objet d'aucune modification.

Le présent article définit les notions de service numérique et de fournisseurs de service numérique en reprenant celles figurant à l'article 4 de la directive (UE) 2016/1148 précitée du 6 juillet 2016, dite directive « *NIS* ».

En application du **1° du présent article**, serait entendu, par service numérique, tout service fourni à titre non gracieux, à distance et par voie électronique, à une personne qui en fait la demande.

Aux termes du **2° du présent article**, un fournisseur de service numérique désignerait toute personne morale fournissant l'un des services suivants :

– un service de place de marché en ligne, qui permet à des consommateurs ou à des professionnels de conclure des contrats de vente ou des services en ligne avec des professionnels (***a***) ;

– un moteur de recherche en ligne, dont la fonction est de permettre aux utilisateurs d'effectuer des recherches sur Internet (***b***) ;

– un service d'informatique en nuage (mieux connu sous l'appellation anglaise « *cloud* »), qui permet l'accès à distance et depuis n'importe quel poste informatique connecté à Internet à un ensemble de ressources partagées (***c***).

Dès lors qu'aucune disposition ne prévoit une liste nominative des fournisseurs de service numérique, comme c'est le cas pour les opérateurs de

services essentiels [(1)], le présent article permet aux personnes morales concernées de savoir si elles se trouvent ou non dans le champ d'application de la loi.

À l'initiative de son rapporteur, la commission des Lois du Sénat a adopté un amendement procédant à la correction d'une erreur de référence au sein du code de la consommation.

*

* *

*La Commission **adopte** l'article 10 **sans modification**.*

Article 11

Champ d'application des dispositions du chapitre III

Résumé du dispositif et effets principaux :

Le présent article précise le champ d'application des dispositions prévues par le chapitre III à l'égard des fournisseurs de service numérique.

Dispositions de la directive concernée : article 18

Modifications apportées au Sénat :

Le Sénat a rendu obligatoire, pour un fournisseur qui offrirait ses services sur le territoire français, de désigner un représentant, dès lors qu'il n'en aurait pas déjà fait de même dans un autre État membre. Il a par ailleurs complété l'article afin de préciser qu'entrent dans le champ d'application du chapitre III les entreprises ayant leur établissement principal en France.

Modifications apportées par votre commission des Lois :

Cet article a fait l'objet d'un amendement de précision de votre rapporteur.

1. Le dispositif proposé

Le **I du présent article** transpose en droit français les 1 et 2 de l'article 18 de la directive (UE) 2016/1148 précitée du 6 juillet 2016, dite directive « *NIS* », relatifs au champ d'application territorial. La directive prévoit notamment une disposition selon laquelle « *le fournisseur de service numérique est considéré comme relevant de la compétence de l'État membre dans lequel le représentant est établi* », ce qui est indispensable pour éviter des doublons réglementaires ou au contraire des vides juridiques s'agissant des fournisseurs de service numérique (FSN) présents dans plusieurs pays de l'Union européenne. En conséquence le premier alinéa du présent article précise que sont soumis aux obligations du projet de loi les FSN qui offrent leurs services dans l'Union et qui ont établi leur siège

(1) Cf. commentaire de l'article 5.

social en France ou qui, dans le cas où ils ne seraient pas établis dans l'Union, ont désigné à cet effet un représentant sur le territoire national.

Le **II du présent article** prévoit – comme l'impose l'alinéa 11 de l'article 16 de la directive « *NIS* » – que les dispositions du chapitre III sur la sécurité des réseaux et systèmes d'information des FSN 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.

2. Les modifications apportées par le Sénat

Le rapporteur du Sénat, M. Philippe Bonnecarrère, a relevé que la directive « *NIS* » d'une part ne prévoit aucun mécanisme juridique permettant aux États membres de s'assurer que les FSN établis hors de l'Union européenne se sont bien déclarés dans un État membre et, d'autre part, ne définit pas l'autorité judiciaire compétente chargée de poursuivre et de sanctionner les fournisseurs qui ne respecteraient pas cette obligation de déclaration. Ainsi, dans le cas d'un fournisseur qui ne se serait déclaré dans aucun Etat membre, la directive ne permet pas à un État membre d'imposer à ce fournisseur de service numérique de se déclarer dans cet État.

Cette situation crée un vide juridique certain sur lequel le Gouvernement a alerté la Commission européenne.

Par un amendement de son rapporteur, la commission des Lois du Sénat a donc rendu obligatoire, pour un fournisseur qui offrirait ses services sur le territoire français, de désigner un représentant, dès lors qu'il n'en aurait pas déjà fait de même dans un autre État membre.

La commission des Lois a par ailleurs complété le premier alinéa de l'article, afin de préciser, comme le prévoit l'article 18 de la directive « *NIS* », qu'entrent également dans le champ d'application du projet de loi les entreprises ayant leur établissement principal en France.

3. Les modifications apportées par votre commission des Lois

À l'initiative de votre rapporteur, la Commission a adopté un amendement visant à limiter l'application du I du présent article aux fournisseurs de service numérique établis hors de l'Union européenne conformément à l'article 18.2 de la directive.

*

* *

*La Commission **adopte** l'amendement de précision CL50 du rapporteur.*

Puis elle est saisie de l'amendement CL14 de Mme Danièle Obono.

M. Ugo Bernalicis. Nous proposons de déterminer par arrêté ministériel les secteurs de service numérique pouvant être exclus du champ d'application du présent article, indépendamment de la taille des entreprises. Exempter automatiquement toutes celles de moins de cinquante salariés et réalisant un chiffre d'affaires de moins de 10 millions d'euros de l'obligation de désigner un représentant ou une représentante auprès de l'ANSSI paraît totalement inadapté à la réalité du numérique et aux enjeux de la cybersécurité. Les critères choisis ne nous semblent pas pertinents en matière de risques et de sécurité. Notre amendement vise à ce que l'on identifie plutôt des domaines non vulnérables, non sensibles ou non stratégiques qui seraient exclus du champ d'application. Il ne faut pas penser les enjeux du numérique en reprenant de vieilles grilles de lecture, inopérantes et *de facto* inefficaces.

M. le rapporteur. Je suis sensible à cette argumentation. Ce que vous proposez viendra probablement dans un avenir relativement proche ; mais pour l'heure, il s'agit de transposer une directive dont l'article 16 prévoit notamment que les entreprises de moins de cinquante salariés et réalisant moins de 10 millions d'euros de chiffre d'affaires ne sont pas concernées… Par conséquent, avis défavorable.

Mme Laurence Vichnievsky. Permettez-moi de faire une observation générale. L'article 11 conditionne la possibilité d'engager des poursuites pénales contre les personnes morales. Ce n'est pas seulement une question technique, comme le montre le cas de Ryanair, dont il a beaucoup été question. Il est très difficile de poursuivre cette société en France, car elle n'y a pas de représentant légal. J'ai lu avec attention les commentaires du rapporteur du Sénat, dont chacun sait à quel point les travaux sont précis, rigoureux, et combien ils nous apportent, mais j'ai le sentiment que la difficulté n'est pas réglée. Je le dis avec humilité, car je n'ai pas pu creuser suffisamment le sujet. J'ai cependant noté qu'un fournisseur de services, notamment américain, qui n'a pas déclaré de représentant dans notre pays et qui n'a pas de filiale dans un État européen pourra assez facilement échapper à d'éventuelles poursuites. Je pose la question, car je n'ai pas de réponse. Des obligations non sanctionnées n'ayant pas beaucoup de portée, le rapporteur peut-il nous éclairer sur ce point ? Je crains qu'il n'y ait une difficulté pour certains fournisseurs de services.

M. le rapporteur. Vous soulevez une question essentielle, qui a fait l'objet de discussions approfondies en amont, lors du débat au Sénat, avec les ministères, mais aussi avec la Commission européenne. Dans l'immédiat, je souscris à la proposition retenue par le Sénat : tout fournisseur doit procéder à la désignation d'un représentant établi sur le territoire national auprès de l'ANSSI. On remédie ainsi à l'insécurité qui pouvait résulter de la rédaction initiale. Le Gouvernement a été sensible à la question et a souscrit, pour le moment, à cette proposition.

M. Ugo Bernalicis. Je voudrais réagir, monsieur de rapporteur, à ce que vous m'avez dit à propos des seuils. Ce n'est pas parce que la directive prévoit

qu'elle ne s'applique pas aux entreprises de moins de cinquante salariés et réalisant moins de 10 millions d'euros de chiffre d'affaires que l'on ne peut rien décider en ce qui les concerne. Ce n'est pas contradictoire. La directive ne dit pas que nous n'avons pas le droit d'appliquer des normes à ces entreprises. Je ne comprends donc pas bien l'argument. Vous pouvez nous dire que vous êtes contre la surtransposition, mais c'est une autre affaire.

Par ailleurs, nous souhaitons que les poursuites ne visent pas seulement les dirigeants, mais aussi les entreprises. C'est le sens d'un prochain amendement.

Suivant l'avis défavorable du rapporteur, la Commission ***rejette*** *l'amendement.*

Elle ***adopte*** *ensuite l'article 11* ***modifié.***

Article 12

Obligations des fournisseurs de service numérique en matière de protection des réseaux et systèmes d'information

Résumé du dispositif et effets principaux :

Le présent article détermine les obligations s'imposant aux fournisseurs de service numérique en matière de sécurité des réseaux et des systèmes d'information.

Dispositions de la directive concernée : article 16

Modifications apportées au Sénat :

Le Sénat a adopté un amendement précisant les domaines dans lesquels les fournisseurs de service numérique sont tenus prendre des mesures techniques et organisationnelles de gestion des risques. Il a par ailleurs opéré diverses améliorations rédactionnelles par voie d'amendement.

Modifications apportées par votre commission des Lois :

Cet article n'a fait l'objet d'aucune modification.

1. Le dispositif proposé

L'article 16 de la directive (UE) 2016/1148 précitée du 6 juillet 2016, dite directive « *NIS* », dispose que « [l]*es 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. »

Votre rapporteur observe que ce régime est moins strict que celui applicable aux opérateurs de services essentiels (OSE), qui doivent 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. 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*. [(1)] » Cela parait pertinent dès lors que la sensibilité de ces FSN est moindre que celle des OSE.

2. Les modifications apportées par le Sénat

À l'initiative de son rapporteur, la commission des Lois du Sénat a adopté un amendement précisant que les FSN sont tenus de prendre des mesures techniques et organisationnelles dans cinq domaines, qui sont ceux édictés à l'article 16 de la directive « *NIS* » : 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, le respect des normes internationales.

Elle a par ailleurs opéré diverses améliorations rédactionnelles par voie d'amendement.

*

* *

La Commission ***adopte*** *l'article 12* ***sans modification****.*

(1) Cf. commentaire de l'article 6.

Article 13
Obligation de déclaration d'incidents

Résumé du dispositif et effets principaux :

Le présent article prévoit, à l'égard des fournisseurs de service numérique, une obligation de signalement de tout incident affectant les réseaux et systèmes d'information et un encadrement des conditions de la publicité donnée à ces incidents.

Dispositions de la directive concernée : article 16

Modifications apportées au Sénat :

Le Sénat a transféré du Premier ministre à l'autorité administrative la responsabilité de communiquer sur les incidents affectant les FSN.

Modifications apportées par votre commission des Lois :

Cet article a fait l'objet d'un amendement rédactionnel de votre rapporteur.

1. Le dispositif proposé

Les 3 et 4 de l'article 16 de la directive (UE) 2016/1148 précitée du 6 juillet 2016, dite directive « *NIS* », sont relatifs à l'obligation de déclaration d'incidents affectant les réseaux et systèmes d'information ayant un impact significatif sur la fourniture de services numériques.

Le dispositif prévu au **I du présent article** est à cet égard le miroir de celui prévu à l'article 7 du projet de loi, à plusieurs différences près :

– il ne vise que les incidents ayant un impact significatif, à l'exclusion des incidents qui seraient susceptibles d'en avoir un [(1)] ;

– les fournisseurs de service numérique (FSN) ne seraient tenus de déclarer les incidents que « *lorsque les informations dont ils disposent* » montrent que ces incidents ont un impact significatif sur leur fourniture ;

– les critères permettant de qualifier le caractère significatif de l'impact sont plus précisément définis ; si l'on retrouve le nombre d'utilisateurs, la zone géographique et la durée, sont en revanche ajoutés la gravité de la perturbation du fonctionnement du service et l'ampleur de son impact sur le fonctionnement de la société ou de l'économie.

Le **II du présent article** fixe les conditions dans lesquelles l'autorité administrative peut être autorisée à communiquer sur un incident affectant un FSN. Celles–ci sont plus étendues que dans le cas des opérateurs de services

(1) Cf. commentaire de l'article 7.

essentiels (OSE) puisque le Premier ministre pourrait contraindre le fournisseur à le faire. Les finalités autorisant une information sont elles aussi plus larges puisqu'elles peuvent être justifiées par tout motif d'intérêt général.

En application de l'alinéa 6 de l'article 16 de la directive « *NIS* », si un incident avait un impact transfrontalier et touchait plusieurs États membres, le Premier ministre serait autorisé à informer les autorités compétentes de ces autres États, qui, eux-mêmes, pourraient le rendre public.

2. Les modifications apportées par le Sénat

Afin d'aligner la rédaction de l'article 13 sur celle de l'article 7, la commission des Lois du Sénat a adopté un amendement de son rapporteur procédant à plusieurs précisions rédactionnelles.

Pour les mêmes raisons que celles exposées à l'article 7 relatif aux OSE, le Sénat a transféré du Premier ministre à l'autorité administrative compétente la responsabilité de communiquer sur les incidents affectant les FSN.

*

* *

*La Commission **adopte** l'amendement de précision rédactionnelle CL26 du rapporteur.*

*Puis elle **adopte** l'article 13 **modifié**.*

Article 14
Modalités de contrôle

Résumé du dispositif et effets principaux :

Le présent article détermine les modalités de contrôle des obligations imposées aux fournisseurs de service numérique en matière de sécurité des réseaux et systèmes d'information.

Dispositions de la directive concernée : article 17

Modifications apportées au Sénat :

Le Sénat a modifié cet article de manière à préciser la procédure d'injonction administrative, pour les mêmes raisons que celles exposées à l'article 8.

Modifications apportées par votre commission des Lois :

Cet article a fait l'objet d'un amendement de précision de votre rapporteur.

Cet article transpose en droit français les 1 et 2 de l'article 17 de la directive (UE) 2016/1148 précitée du 6 juillet 2016, dite directive « *NIS* ». On observe que si cet article présente un certain nombre de similarités avec l'article 8 [(1)] sur les modalités de contrôle des opérateurs de services essentiels (OSE), il s'en distingue par une plus grande souplesse.

Ainsi, si le **premier alinéa du présent article** prévoit effectivement que le Premier ministre puisse soumettre un fournisseur de service numérique (FSN) à des contrôles destinés à vérifier le respect des obligations prévues par le projet de loi, ceux-ci ne sont possibles que dans l'hypothèse où le chef du Gouvernement serait informé que ce FSN ne satisfait pas à l'une de ces obligations.

En raison du caractère transfrontalier de l'activité des FSN, cet alinéa prévoit également un dispositif d'information et de coopération avec les autres États membres concernés.

Les **deuxième et troisième alinéas du présent article** précisent les modalités de mise en œuvre des contrôles, qui s'opèreront dans des conditions identiques à celles prévues à l'article 8.

Enfin, le **quatrième alinéa du présent article** prévoit, comme à l'article 8, que les FSN seraient susceptibles de faire l'objet d'une mise en demeure de se conformer aux obligations qui leur incombent.

Par un amendement de son rapporteur, la commission des Lois du Sénat a réécrit ce dernier alinéa de manière à préciser la procédure d'injonction administrative, pour les mêmes raisons qu'à l'article 8.

*

* *

*La Commission **adopte** l'amendement rédactionnel CL33 du rapporteur.*

*Elle **adopte** ensuite l'article 14 **modifié**.*

(1) Cf. commentaire de l'article 8.

Article 15
Sanctions pénales

Résumé du dispositif et effets principaux :

Le présent article détermine le régime de sanctions pénales applicable aux fournisseurs de service numérique en cas de manquement à leurs obligations.

Dispositions de la directive concernée : article 21

Modifications apportées au Sénat :

Par cohérence le Sénat a apporté la même modification de précision qu'à l'article 9.

Modifications apportées par votre commission des Lois :

Cet article n'a fait l'objet d'aucune modification.

L'article 21 de la de la directive (UE) 2016/1148 précitée du 6 juillet 2016, dite directive « *NIS* », prévoit que 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*. »

En conséquence, le présent article institue trois infractions, de même nature que celles créées par l'article 9 du projet de loi à l'encontre des opérateurs de services essentiels. Les amendes applicables seraient toutefois moins élevées, conformément à l'exigence de proportionnalité. Ainsi :

– l'infraction prévue au **premier alinéa**, qui sanctionne le fait de ne pas se conformer aux mesures de sécurité des réseaux et des systèmes d'information [(1)], est sanctionnée d'une amende de 75 000 euros ;

– l'infraction prévue au **deuxième alinéa**, qui pénalise le fait de ne pas satisfaire à l'obligation de déclaration d'incidents à l'ANSSI [(2)], est passible d'une amende de 50 000 euros ;

– l'infraction prévue au **troisième alinéa**, qui réprime le fait de faire obstacle aux opérations de contrôle des obligations de sécurité, est punie d'une amende de 100 000 euros [(3)].

La commission des Lois du Sénat a apporté la même modification de précision qu'à l'article 9.

---

(1) Cf. commentaire de l'article 12 du projet de loi.

(2) Cf. commentaire de l'article 13 du projet de loi.

(3) Cf. commentaire de l'article 14 du projet de loi.

*

* *

La Commission examine l'amendement CL16 de M. Ugo Bernalicis.

Mme Danièle Obono. Cet amendement, comme le CL13 à l'article suivant, s'inscrit dans la même logique que les précédents. Ainsi que l'a indiqué mon collègue Ugo Bernalicis, il s'agit d'élargir le cadre des amendes infligées en cas de manquement.

M. le rapporteur. Même avis défavorable.

*La Commission **rejette** l'amendement.*

*Suivant l'avis défavorable du rapporteur, la Commission **rejette** ensuite l'amendement CL13 de Mme Danièle Obono.*

*Puis la Commission **adopte** l'article 15 **modifié**.*

Après l'article 15

La Commission examine l'amendement CL9 de Mme Danièle Obono.

Mme Danièle Obono. Cet amendement concerne les chasseurs et les chasseuses de failles qui contribuent quotidiennement à renforcer la cybersécurité, à la différence des sociétés en conseil informatique, celles-ci intervenant de manière conjoncturelle quand un risque est pressenti. On ira dans le sens d'une meilleure sécurité en offrant une prime, une sorte de *bug bounty*, à celles et ceux qui détectent des dysfonctionnements dans les systèmes informatiques, au-delà même de certains opérateurs qui relèvent du code de la défense et sont dans l'immédiat visés par l'amendement.

C'est une façon innovante d'encourager et de mettre à contribution les nombreux et nombreuses bénévoles qui pourraient contribuer, chaque jour, à rendre notre système plus fort. Ces acteurs ont des formations différentes et connaissent d'autres techniques, parfois moins académiques et plus créatives – je sais à quel point la majorité adore libérer les énergies et la créativité. *(Sourires.)* Nous serons ainsi plus réactifs et réactives sur le terrain.

Avec cet amendement, les chasseurs et les chasseuses de failles pourront bénéficier d'un statut juridique qui les protégera et les encouragera à participer à la construction de dispositifs informatiques plus robustes, alors qu'ils et elles naviguent pour l'instant entre la légalité et l'illégalité. Leurs compétences seront utilisées non pour déconstruire, mais pour consolider les dispositifs actuels.

M. le rapporteur. Avis défavorable. Une fois encore, cet argument très intéressant mériterait probablement d'être étudié, mais dans un autre contexte. Je rappelle qu'en vertu d'une décision du Conseil constitutionnel datant de 2015, les

amendements déposés sur un projet de loi visant à transposer une directive européenne doivent, pour présenter un lien direct avec le texte, concerner la transposition de directives communautaires en lien avec la matière. Or ce n'est pas le cas avec vos amendements. En sortant du cadre strict de la transposition, nous excédons nos compétences. C'est donc partie remise même s'il était utile que le débat puisse avoir lieu.

M. Ugo Bernalicis. Je ne comprends plus. L'idée est qu'il pourrait exister des *hackers* bienveillants, les chasseurs de failles. Comme tous les autres hackers, ils se livrent à des attaques, mais dans le but de détecter, au bout du compte, et de combler les brèches. Vous ne pouvez pas soutenir qu'il n'y a pas de lien avec la cybersécurité – le lien est même très direct. Il s'agit de trouver les failles, avec ceux qui savent le faire, en recourant à des techniques parfois similaires à celles des pirates. Notre amendement instaure une sorte de prime afin de créer un système participatif, communautaire ou contributif – peu importe le terme – en matière de cybersécurité. Vous ne pouvez donc pas nous dire que cela n'entre pas dans le cadre du sujet. Sinon, il y aurait beaucoup de hors sujet…

La Commission ***rejette*** *l'amendement.*

Puis elle examine l'amendement CL10 de Mme Danièle Obono.

Mme Danièle Obono. Nous allons peut-être en rajouter une petite couche : nous allons clairement dans le sens du texte – il n'est pas question ici, pour le coup, d'opposition idéologique à ce que vous proposez au prétexte qu'il s'agirait d'une régression, d'une atteinte à l'intérêt général, etc. Il s'agit vraiment d'essayer d'avancer ensemble dans un domaine que la majorité elle-même, elle l'a assez dit sur tous les tons et sur tous les plateaux de télévision, considère comme important. Nous pourrions nous montrer inventifs et faire ce que font d'autres États. On sait qu'en matière de cybersécurité, ce sont souvent les initiatives individuelles qui permettent d'avancer et qui sont ensuite utilisées pour servir le bien commun.

L'amendement CL10, dans la suite logique du précédent qui visait à définir un statut et à faire en sorte que les chasseurs et les chasseuses de failles participent à la cybersécurité collective, pose le problème des primes de dysfonctionnement, appelées *bug bounty*, et de la prise au sérieux du travail réalisé. Nous insistons donc sur la nécessité de prendre en compte ce débat qui est complètement dans le sujet – et je dirai même : qu'est-ce qui pourrait être plus dans le sujet ?

M. le rapporteur. Ma réponse repose sur les mêmes arguments que précédemment. Sur le fond, nous sommes d'accord : il faut réfléchir à un statut pour les chasseurs de failles ; mais nous avons un problème de forme. Le Conseil constitutionnel, dans son communiqué de presse au sujet de sa décision n° 2015-719 DC du 13 août 2015, précise que, « *s'agissant d'une loi ayant pour objet de transposer des directives communautaires en matière pénale, des dispositions*

ayant pour objet de transposer des directives européennes relatives à la matière pénale autres que celles figurant dans le projet de loi initial présentent un lien direct avec le texte déposé. En revanche, des dispositions pénales n'ayant pas pour objet de transposer une directive européenne ne présentent pas un tel lien ». Votre amendement est donc hors sujet.

M. Erwan Balanant. Le rapporteur vient de l'expliquer très clairement : c'est juste une question de forme juridique, ce qui ne signifie pas que les questions que vous soulevez ne soient pas intéressantes – elles sont même pour moi primordiales. En effet, ceux qui chassent les failles sont aujourd'hui parfois attaqués voire condamnés pour des actes qui, s'ils ne relèvent tout de même pas du salut public – il ne faut pas exagérer –, n'en participent pas moins à notre sécurité. Il faudra donc trouver, à un moment ou à un autre, une manière d'intégrer ces questions dans un texte qui ne soit pas une transposition de normes de l'Union européenne mais bien le fruit de nos propres travaux.

M. Raphaël Schellenberger. Regretter l'absence de liberté du législateur est une chose, mais vous ne pouvez pas tirer prétexte de la transposition de directives de l'Union européenne pour nous expliquer à quel point vous rejetez l'idée même de la construction européenne, tout en voulant faire de chaque texte émanant de l'Union une tribune pour avancer vos propositions.

La décision du Conseil constitutionnel protège le législateur national. Quand on transpose un texte émanant de l'Union européenne, c'est ce texte-là qu'on transpose ; si l'on décide d'aller au-delà de ce qui est expressément prévu, alors c'est un texte de droit national et non plus un texte transposé du droit européen. Il faut bien comprendre cette logique de protection constitutionnelle, vis-à-vis de ce que d'autres ont appelé la surtransposition des directives européennes.

Sur le fond, votre amendement est intéressant même si, à mon avis, vous allez parfois un peu trop loin. La question est ici celle de la citoyenneté numérique ; dès lors, avant d'agiter la revendication d'un statut ou d'un droit, il faut s'interroger sur les notions d'engagement et de devoir.

Mme Danièle Obono. Vous comprendrez mieux bientôt, cher collègue, quelles sont nos positions sur l'Union européenne, et elles ne sont pas aussi caricaturales que vous le croyez. Nous essayons pour notre part de construire autre chose. Et vous noterez que depuis le début de la discussion, nous votons les articles parce que nous pensons que ce texte comporte des éléments positifs. Ensuite, mais vous ne l'avez peut-être pas lu, l'amendement demande un rapport. Dernier point, ce que nous proposons ne relève pas du droit pénal : nous demandons un statut. Encore une fois, il ne s'agit pas d'une question idéologique. Argumentez sur ce que nous proposons !

*La Commission **rejette** l'amendement.*

Puis elle en vient à l'amendement CL12 de M. Ugo Bernalicis.

M. Ugo Bernalicis. Nous souhaitons que le Parlement soit informé des points faibles des réseaux matériels français et européens concernant le risque d'espionnage et de fuite de données. La représentation nationale et les citoyens doivent pouvoir apprécier les efforts faits par les services de l'État en matière de préservation matérielle et physique de la souveraineté des données. L'espionnage est une réalité : le lanceur d'alerte Edward Snowden en a fait la démonstration en révélant l'existence de différents programmes d'espionnage de masse exécutés sur de grands câbles internet sous-marin mondiaux transitant notamment par le Royaume-Uni. Il faudrait adopter une approche multiscalaire de la cybersécurité, à savoir à la fois nationale et européenne, afin que nous puissions vraiment protéger nos données.

On nous reproche de nous servir de l'examen de ce texte comme d'une tribune. Ce n'est pas le cas – à moins de considérer que nos amendements relèvent de la fonction tribunitienne et ainsi servent l'intérêt général… Nous n'avons rien contre les directives européennes en soi – du reste, nous avons voté tous les articles depuis le début de la discussion. Il n'y a donc aucune incohérence de notre part. Et lorsque nous proposerons une autre Europe, nous aurons prévu les règles de cybersécurité, ne vous inquiétez pas !

Suivant l'avis défavorable du rapporteur, la Commission ***rejette*** *l'amendement.*

TITRE II
DISPOSITIONS RELATIVES AU CONTRÔLE DE L'ACQUISITION ET DE LA DÉTENTION D'ARMES

Le titre II du projet de loi se compose de sept articles – six présents dans la rédaction initiale, un septième issu d'un amendement du rapporteur du Sénat. Il a pour objet l'adaptation du droit français aux nouvelles prescriptions du droit européen en matière d'armes à feu.

L'**harmonisation des règles d'acquisition et de détention d'armes à feu** à l'échelle européenne a commencé le 18 juin 1991 avec la directive 91/477/CEE du Conseil. Ce texte établissait les exigences minimales imposées par les États membres pour chaque catégorie d'armes et les conditions de transfert entre États membres. La directive modificative 2008/51/CE du 21 mai 2008 a renforcé les éléments liés à la sécurité et mis le droit européen en conformité avec le droit onusien [(1)].

Plus récemment, dans un **contexte de lutte contre le terrorisme international**, la directive (UE) 2017/853 du Parlement européen et du Conseil du 17 mai 2017 a retenu une logique de renforcement des mesures de sécurité. Elle

(1) 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, adopté par la résolution 55/255 de l'Assemblée générale des Nations Unies le 31 mai 2001 et entrée en vigueur le 3 juillet 2005.

s'inscrit dans le prolongement de la « **Déclaration de Paris** » n° 5322/15 du 11 janvier 2015 dans laquelle, à la suite immédiate de la vague d'attentats qui venait de frapper la France, les ministres de l'intérieur et de la justice de l'Union européenne ont notamment affirmé leur détermination à lutter contre la circulation illégale d'armes à feu sur le territoire de l'Union. Le Conseil « Justice et affaires intérieures » des 12 et 13 mars 2015 a ensuite invité la Commission à proposer de nouveaux moyens pour lutter contre ce trafic [(1)]. Le Parlement européen s'était prononcé dans le même sens dans une résolution du 11 février 2015.

La Commission européenne a présenté une proposition de directive le 18 novembre 2015. **Cette initiative a reçu le soutien de l'Assemblée nationale** [(2)].

L'article 2§1 de la directive du 17 mai 2017 prévoit que les États membres procèdent à sa **transposition au plus tard le 14 septembre 2018**.

Le régime des armes à feu relève pour l'essentiel du domaine réglementaire. Toutefois, certaines dispositions de la directive du 17 mai 2017 nécessitent une transposition par voie législative :

– la disparition de la catégorie D1, soumise à enregistrement ;

– le nouveau régime des reproductions d'armes historiques ;

– l'instauration d'un contrôle administratif pour les courtiers d'armes de catégorie C ;

– les dérogations à l'interdiction d'acquisition et de détention d'armes de catégorie A ;

– l'interdiction de la livraison au domicile d'armes achetées par correspondance ;

– la surveillance des transactions jugées suspectes par les armuriers.

Les trois premières dispositions, qui requièrent un grand nombre de coordinations, font l'objet des articles 16, 17, 19, 20, 21 et 21 *bis* du titre II du projet de loi. Les trois dernières sont transposées à l'article 18.

---

(1) Communiqué de presse 7178/15.

(2) Résolution européenne sur la proposition de directive du Parlement et du Conseil relative aux armes à feu, 11 juin 2016, TA n° 751.

Article 16

(art. L. 311-2 et L. 311-4 du code de la sécurité intérieure)

Suppression du régime d'enregistrement des armes à feu et contrôle administratif des reproductions d'arme historique

Résumé du dispositif et effets principaux :

L'article 16 du projet de loi supprime la catégorie d'armes D1 soumise à enregistrement auprès de l'autorité administrative, conformément à la directive européenne du 17 mai 2017. Il confie également au pouvoir réglementaire le soin de soumettre à déclaration l'acquisition et la détention des reproductions d'armes historiques ayant bénéficié pour leur élaboration de techniques modernes améliorant leur durabilité et leur précision.

Modifications apportées par le Sénat :

Outre diverses coordinations, le Sénat a maintenu dans le domaine de la loi le classement des reproductions d'arme historique en catégorie D, sauf celles présentant une dangerosité avérée.

Modifications apportées par la commission des Lois :

La Commission a rétabli la compétence du pouvoir réglementaire pour le classement des reproductions d'armes historiques, conformément à l'analyse du Conseil d'État et aux prescriptions de la directive du 17 mai 2017.

1. L'état du droit

L'article L. 311-2 du code de la sécurité intérieure [(1)] répartit en **quatre catégories** les armes et matériels de guerre ainsi que leurs éléments et munitions.

ACQUISITION ET DÉTENTION D'ARMES

Régimes européen et français avant la directive du 17 mai 2017 et sa transposition

	Droit de l'Union européenne	Droit français
Catégorie A	Armes à feu interdites	Matériels de guerre et armes soumis à un régime d'interdiction d'acquisition et de détention, sauf dérogations fixées par la loi.
Catégorie B	Armes à feu soumises à autorisation	Armes soumises à autorisation
Catégorie C	Armes à feu soumises à déclaration	Armes soumises à déclaration
Catégorie D	Autres armes à feu sans contrôle administratif	**Catégorie D1** Armes soumises à enregistrement
		Catégorie D2 Armes sans contrôle administratif

(1) Cet article résulte de la loi n° 2012-304 du 6 mars 2012 relative à l'établissement d'un contrôle des armes modernes.

Chaque catégorie fait l'objet d'un **régime particulier d'acquisition et de détention** en fonction du degré de dangerosité des armes considérées. Si la définition des catégories est de rang législatif, l'affectation des différentes armes en leur sein relève du pouvoir règlementaire (1).

Cette catégorisation reprend essentiellement le classement des armes à feu défini au niveau européen par la directive 91/477/CEE du 18 juin 1991 relative au contrôle de l'acquisition et de la détention d'armes. Cependant, contrairement au droit européen, **le droit français ne se limite pas aux armes à feu** : il inclut les autres sortes d'armes ainsi que les armes d'alarme, de collection et neutralisées.

2. Les dispositions du projet de loi

a. La fin du régime d'enregistrement des armes à feu

Dans une perspective de renforcement du contrôle public sur l'acquisition, la détention et la circulation des armes à feu, la directive du 17 mai 2017 précitée supprime **la catégorie D du droit européen**, qui ne prescrivait aucune supervision administrative, **et transfère les équipements qui en relevaient en catégorie C**, qui exige des propriétaires une déclaration à l'autorité administrative. Sont concernées par ce durcissement de la règlementation les « *armes à feu longues à un coup par canon lisse* », soit la plupart des **armes de chasse**.

La France s'était dotée d'un **régime plus strict que le droit européen**. Les armes concernées sont aujourd'hui classées en catégorie D1 et soumises au régime de l'enregistrement. Leur basculement en catégorie C doit logiquement aboutir à la **suppression de la catégorie D1**, qui se perpétuerait dans le cas contraire sous la forme d'une coquille vide.

ACQUISITION ET DÉTENTION D'ARMES

Régimes européen et français après la directive du 17 mai 2017 et sa transposition

	Droit de l'Union européenne	Droit français
Catégorie A	Armes à feu interdites	Matériels de guerre et armes soumis à un régime d'interdiction d'acquisition et de détention, sauf dérogations fixées par la loi
Catégorie B	Armes à feu soumises à autorisation	Armes soumises à autorisation
Catégorie C	Armes à feu soumises à déclaration	Armes soumises à déclaration
Catégorie D		Armes non soumises au droit européen et sans contrôle administratif

La disparition de la catégorie D1 laisse cependant subsister, en droit français, la catégorie D2 – qui devient de ce fait une **nouvelle catégorie D**. Toutes

(1) Article R. 311-2 du code de la sécurité intérieure.

les références à la catégorie D ne doivent donc pas disparaître du droit positif, mais seulement celles visant les armes soumises à enregistrement.

Il convient de souligner que **la suppression du régime d'enregistrement aura peu d'impact sur les possesseurs d'armes concernées**. En effet, les contrôles administratifs appliqués aux catégories C et D1 ont été fortement rapprochés par 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. Depuis lors, la détention d'armes de catégories C et D1 est pareillement conditionnée à l'absence de mention de certaines infractions sur le bulletin n° 2 du casier judiciaire [(1)]. Seule l'exigence d'un certificat médical distingue aujourd'hui les deux catégories – et encore l'article L. 312-6 du code de la sécurité intérieure en dispense-t-il les titulaires d'une licence de tir ou d'un permis de chasse.

COMPARATIF DES RÉGIMES APPLICABLES AUX ARMES DE CATÉGORIE C ET D1

	Catégorie C	**Catégorie D**
Bulletin n° 2 du casier judiciaire exempt d'une condamnation prévue à l'article L. 312-3 CSI	Oui	Oui
Absence de comportement dangereux (L. 313-3 CSI)	Oui	Oui
Document attestant du bien-fondé de l'acquisition d'une arme	Licence de chasse, licence de tir, carte de collectionneur (art. L. 312-4-1 CSI)	Licence de chasse, licence de tir (art. R. 312-53 CSI)
Certificat médical	Oui, sauf licence de chasse ou de tir (art. 312-6 CSI)	Non
Déclaration ou enregistrement auprès de l'autorité administrative	Oui (art. L. 312-4-1 CSI)	Oui (art. R. 312-56 CSI)

Source : commission des Lois du Sénat.

Quant aux modalités d'entrée en vigueur de ces dispositions pour les personnes déjà titulaires d'une arme aujourd'hui classée en catégorie D1, trois situations seront à distinguer :

– les armes acquises **avant le 1er décembre 2011**, date de transposition de la directive du 21 mai 2008 précitée en droit français par le décret n° 2011-1253 du 7 octobre 2011 modifiant le régime des matériels de guerre, armes et munitions, bénéficient d'une clause d'antériorité qui **exempte leur propriétaire de toute démarche administrative** ;

– les armes acquises **entre le 1er décembre 2011 et le 13 juin 2017**, date d'entrée en vigueur de la directive du 17 mai 2017, ne sont pas soumises à une formalité administrative pour leur détention en France. Toutefois, leur transport

(1) Article L. 312-3 du code de la sécurité intérieure.

sur le territoire d'un autre État membre nécessitera une démarche administrative pour l'obtention d'un titre de catégorie C ;

– les armes acquises **à partir du 13 juin 2017** sont soumises au régime de déclaration de la catégorie C. Les détenteurs devront régulariser leur situation, sauf à ce que le pouvoir réglementaire prévoie le basculement automatique d'un régime à l'autre en assimilant les récépissés d'enregistrement et de déclaration.

Les articles 16, 17, 19 et 20 du projet de loi suppriment toute référence à la procédure d'enregistrement de la catégorie D1 au sein du code de la sécurité intérieure. L'article 21 fait de même dans le code de la défense et l'article 21 *bis* dans la loi n° 55-385 du 3 avril 1955 relative à l'état d'urgence.

b. Le durcissement du régime des reproductions d'armes historiques

La directive du 17 mai 2017 précitée intègre dans le droit européen de l'acquisition et de la détention d'armes certains équipements qui en étaient jusque-là exclus en raison de leur faible dangerosité : les **reproductions d'armes historiques** au motif que des « *techniques modernes et susceptibles d'améliorer leur durabilité et leur précision* » ont pu être employées pour leur assemblage [(1)], et les **armes neutralisées**, par crainte de leur réactivation [(2)]. Elles sont désormais **classées en catégorie C** et, à ce titre, soumises à un régime de déclaration.

En droit français, si le classement en catégorie C des armes neutralisées relève du pouvoir réglementaire [(3)], il n'en va pas de même des armes historiques et de leurs reproductions : définies à l'article L. 311-3 du code de la sécurité intérieure [(4)], elles sont classées en catégorie D par l'article L. 311-4 du même code.

Le **2° de l'article 16** du projet de loi autorise le Gouvernement à tirer les **conséquences de l'évolution du droit européen** en renvoyant à un décret en

---

(1) « Lorsque les États membres disposent de législations nationales régissant les armes anciennes, celles-ci ne sont pas soumises à la directive 91/477/CEE. Toutefois, 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. Par conséquent, ces reproductions devraient relever du champ d'application de la directive 91/477/CEE » (considérant n° 27 de la directive du 17 mai 2017).

(2) Art. 10 ter *de la directive précitée.*

(3) L'article R. 311-2 du code de la sécurité intérieure prévoit que l'acquisition et la détention des armes neutralisées sont libres.

(4) Relèvent de la catégorie des armes et matériels historiques et de collection :

1° les armes de modèle antérieur au 1er janvier 1900, sauf dangerosité avérée ;

2° les armes de modèle postérieur au 1er janvier 1900 et énumérées par 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, c'est-à-dire les armes neutralisées ;

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 neutralisés de catégorie A de modèle antérieur au 1er janvier 1946 ;

6° les matériels de guerre neutralisés de catégorie A de modèle postérieur au 1er janvier 1946 énumérés par arrêté du ministre de la défense compte tenu de leur intérêt culturel, historique ou scientifique.

Conseil d'État le soin de classer des armes historiques et leurs reproductions en catégorie C : celles dont la durabilité et la précision auraient été améliorées par des techniques modernes.

L'étude d'impact jointe au projet de loi souligne que « *ce classement législatif constitue une* ***anomalie juridique****, puisque le classement relève du champ réglementaire* ». **Le Gouvernement est d'ailleurs responsable de ladite anomalie** dans la mesure où l'article L. 311-4 du code de la sécurité intérieure n'est pas le fait du Parlement mais de l'ordonnance n° 2013-518 du 20 juin 2013 modifiant certaines dispositions du code de la sécurité intérieure et du code de la défense (parties législatives) relatives aux armes et munitions.

3. Les modifications apportées par le Sénat

Sur proposition du rapporteur, la commission des Lois du Sénat a procédé à **diverses coordinations** pour la suppression de la procédure d'enregistrement des armes à feu de la catégorie D1.

En ce qui concerne le régime applicable aux armes historiques, la commission des Lois a adopté un amendement du rapporteur **maintenant leur classement en catégorie D** – dans la nouvelle catégorie D, équivalente à l'actuelle catégorie D2 – sauf pour celles présentant une **dangerosité avérée** et qui figureraient sur une **liste dressée par décret en Conseil d'État**. Les associations de collectionneurs avaient, en effet, fait part de leur crainte devant la rédaction du Gouvernement, qui leur paraissait remettre en cause également le classement des armes historiques elles-mêmes en catégorie D.

Si le Gouvernement n'a pas sollicité le retour à la rédaction initiale en séance publique, il a néanmoins formulé des **réserves** par la voix de Mme Jacqueline Gourault, ministre auprès du ministre de l'Intérieur, qui a souhaité que « *ces différents points soient revus dans la suite du processus législatif* [(1)] ».

4. La position de votre Commission

La commission des Lois a adopté un **amendement du rapporteur rétablissant la rédaction initiale du projet de loi pour l'article L. 311-4 du code de la sécurité intérieure**, de sorte que le classement des armes et matériels historiques et de collection ainsi que leurs reproductions relève du pouvoir réglementaire. Cette position est conforme à la répartition des domaines législatif et réglementaire résultant des articles 34 et 37 de la Constitution. De plus, la directive ne permet pas, comme le fait l'amendement adopté par le Sénat, de substituer le critère de « *dangerosité avérée* » d'une reproduction à celui de

(1) Séance n° 41 du 19 décembre 2017.

« *recours aux techniques modernes susceptibles d'améliorer leur durabilité et leur précision* » [(1)].

La commission des Lois a cependant veillé à ce que la passion des collectionneurs ne soit pas affectée par les dispositions du projet de loi. Afin d'apaiser les inquiétudes qui se sont manifestées, votre rapporteur a tenu à apporter les **clarifications suivantes** :

– le droit applicable aux **armes neutralisées** demeure **régi par la partie réglementaire** du code de la sécurité intérieure. C'est donc au Gouvernement qu'il appartiendra de prendre les mesures nécessaires à leur classement en catégorie C, dans les conditions prévues par la directive du 17 mai 2017, qui s'attache principalement à ce que soit vérifié le caractère irréversible de cette neutralisation ;

– la directive n'apporte **aucune modification au régime des armes anciennes et de leurs reproductions à l'identique**, qui n'entrent pas dans le classement européen [(2)] et ont vocation à demeurer en catégorie D au sens du droit français ;

– les **armes anciennes neutralisées** seront toujours qualifiées d'« *armes et matériels historiques et de collection* » au sens de l'article L. 311-3 du code de la sécurité intérieure. Elles échappent aux formalités prévues pour l'ensemble des armes neutralisées dès lors que leur neutralisation a eu lieu avant l'entrée en vigueur de la directive du 17 mai 2017 [(3)] ;

– seul a vocation à évoluer le statut des **reproductions d'armes historiques améliorées par des techniques modernes**, en termes de précision ou de durabilité notamment. Ces armes, dont l'apparence évoque l'ancien mais dont les mécanismes sont contemporains, seront classées désormais en catégorie C.

Par ailleurs, il convient de rappeler que **le droit français proscrit par principe le port d'armes de toutes catégories** [(4)]. Cette interdiction vaut aussi bien pour les armes à feu que pour les armes blanches ou les autres types d'armes.

Le **transport « *sans but légitime* » est réprimé** de deux ans d'emprisonnement et de 30 000 euros d'amende pour les armes de catégorie C, d'un an d'emprisonnement et de 15 000 euros d'amende pour les armes de

---

(1) Les divergences entre ces deux critères sont manifestes : un fusil de l'époque napoléonienne reproduit conformément aux standards de l'époque n'a bénéficié d'aucune technique améliorant sa durabilité ou sa précision, mais il reste une arme à la dangerosité avérée. La rédaction du Sénat pourrait aboutir à son classement en catégorie C, ce que la directive du 17 mai 2017 ne prévoit pas.

(2) Aux termes du considérant 27 de la directive du 17 mai 2017 : « Ces armes ne sont pas soumises à la directive 91/477/CEE ».

(3) Art. 10 ter *de la directive précitée.*

(4) Article L. 315-1 du code de la sécurité intérieure.

catégorie D – y compris, donc, les armes blanches et les armes historiques [1]. Le transport est **réputé légitime** pour :

– les **forces de l'ordre** et les agents de sécurité [2] ;

– les participants à une **reconstitution historique** [3] ;

– les titulaires d'une **licence de tir**, d'un **permis de chasser** ou d'une **carte de collectionneur** [4].

Votre rapporteur relève cependant que, si ces dispositions législatives prémunissent les pratiquants de la chasse et du tir sportif contre toute difficulté, il n'en va pas de même des collectionneurs. En effet, la « **carte de collectionneur** » prévue à l'article 5 de la loi n° 2012-304 du 6 mars 2012 relative à l'établissement d'un contrôle des armes moderne, simplifié et préventif devait voir ses conditions d'établissement et de validité précisées par décret en Conseil d'État [5]. Or, près de six ans après la promulgation de la loi, **ce décret reste à paraître**. Cet état du droit place dans une **situation difficile** les amateurs d'armes anciennes, qui remplissent les conditions légales et règlementaires pour les acquérir et les détenir, mais ne pourraient en aucun cas les transporter – ne serait-ce qu'entre l'armurerie et le lieu de la collection. Votre rapporteur a sensibilisé le Gouvernement à cette difficulté, qui devrait être résolue dans la suite du processus législatif.

Enfin, votre rapporteur partage la position du Gouvernement et du Sénat qui, tous deux, ont décliné la possibilité de dérogation ouverte par la directive du 17 mai 2017 pour l'accès des collectionneurs à certaines armes de catégorie A [6]. Il convient de rappeler que **le droit en vigueur autorise la collection des armes des catégories C et D uniquement**, tandis que l'acquisition ou la détention d'armes de catégorie B – et *a fortiori* d'armes de catégorie A – font l'objet d'une interdiction [7]. Il serait **contraire à l'esprit de la directive, et surtout à l'intérêt national** dans une période marquée par une menace terroriste élevée, que le législateur autorise à l'occasion de sa transposition l'acquisition et la détention d'armes semi-automatiques à des collectionneurs qui, jusqu'à présent, n'y avaient pas accès.

---

(1) Ces peines prévues à l'article L. 317-8 du code de la sécurité intérieure sont portées respectivement à cinq ans d'emprisonnement et 75 000 euros d'amende, et à deux ans d'emprisonnement et 30 000 euros d'amende, lorsque le transport sans but légitime est commis en réunion (art. L. 317-9 du même code).

(2) Articles L. 315-1 et L. 315-2 du code de la sécurité intérieure.

(3) Article R. 315-3 du code de la sécurité intérieure.

(4) Article L. 317-9-1 du code de la sécurité intérieure.

(5) Cette disposition figure désormais à l'article L. 312-6-4 du code de la sécurité intérieure.

(6) Article 6, §3, de la directive précitée.

(7) Articles L. 312-4-1 à L. 312-4-3 du code de la sécurité intérieure. Encore l'acquisition d'armes de catégorie C suppose-t-elle la production de la « carte de collectionneur » que le pouvoir réglementaire n'a pas encore créée.

*

* *

La Commission examine l'amendement CL38 du rapporteur.

M. le rapporteur. Cet amendement propose de revenir à la rédaction initiale du texte. La notion de dangerosité avérée, que les sénateurs ont introduite pour répondre aux craintes de certains collectionneurs, est connue en droit mais nous paraît aller à l'encontre des préconisations de la directive qui, pour sa part, fait référence à des armes reconstituées pour lesquelles on a eu recours « *aux techniques modernes susceptibles d'améliorer leur durabilité et leur précision* ». Cette formulation me paraît meilleure. Les collectionneurs ne doivent pas nourrir d'inquiétude particulière puisque le Gouvernement a déjà envoyé des signes forts destinés à les rassurer.

*La Commission **adopte** l'amendement.*

*Puis elle **adopte** l'article 16 **modifié.***

Article 17

(art. L. 312-2, L. 312-3, L. 312-3-1, L. 312-4, L. 312-4-2, L. 312-4-3, L. 312-5, L. 312-11, L. 312-13, L. 312-16 et L. 314-2 du code de la sécurité intérieure)

Durcissement du régime des armes semi-automatiques et coordinations

Résumé du dispositif et effets principaux :

L'article 17 interdit l'acquisition et la détention des armes semi-automatiques, sauf dérogation prévue par la loi. Il procède également à des coordinations dans le code de la sécurité intérieure pour la bonne application des dispositions de l'article 16.

Modifications apportées par le Sénat :

Le Sénat a explicitement exclu que les collectionneurs d'armes puissent bénéficier d'une dérogation pour la détention d'armes de catégorie A. Il a également aligné les conditions de cession de ces armes sur celles des armes de catégorie B.

Modifications apportées par la commission des Lois :

La Commission a créé une infraction de tentative d'acquisition, de cession et de détention des armes de catégorie C. Ceci permettra l'adhésion de la France au Protocole des Nations unies sur les armes à feu.

1. Le classement d'armes de la catégorie B en catégorie A

a. Les stipulations de la directive du 17 mai 2017

La directive du 17 mai 2017 précitée classe en catégorie A – interdiction d'acquisition et de détention – des armes à feu jusqu'à présent soumises au régime d'autorisation de la catégorie B. Trois types d'armes sont visés :

– les **armes automatiques** (1) converties en armes semi-automatiques (2) ;

– les **armes semi-automatiques** pouvant contenir, pour les longues, plus de 10 cartouches, et pour les courtes, plus de 20 cartouches ;

– les **armes longues dont la longueur peut être réduite** à moins de 60 centimètres en repliant ou retirant la crosse sans l'aide d'outils.

Des **dérogations** sont possibles, à la discrétion des États membres, au bénéfice des tireurs sportifs, des professionnels de la vente d'armes à feu, des musées, de collectionneurs enregistrés et contrôlés et d'autres catégories de personnes dans des cas particuliers, exceptionnels et motivés.

b. Les dispositions du projet de loi

Le classement des armes par catégorie relève du **pouvoir réglementaire**, de sorte que le passage de la catégorie B à la catégorie A des armes visées ne nécessite aucune intervention du législateur (3).

Toutefois, les dérogations au principe d'interdiction sont prévues à l'article L. 312-2 du code de la sécurité intérieure aux termes duquel : « *L'acquisition et la détention des matériels de guerre, armes et éléments d'armes relevant de la catégorie A sont interdites, sauf pour les* ***besoins de la défense nationale et de la sécurité publique****. Un décret en Conseil d'État définit les conditions dans lesquelles* ***l'État****, pour les besoins autres que ceux de la défense nationale et de la sécurité publique,* ***les collectivités territoriales et les organismes d'intérêt général ou à vocation culturelle, historique ou scientifique*** *peuvent être autorisés à acquérir et à détenir des matériels de guerre, armes et éléments d'armes de catégorie A. Il fixe également les conditions dans lesquelles certains matériels de guerre peuvent être acquis et détenus* ***à fin de collection,***

(1) Une arme automatique est capable de tirer des projectiles par rafales, les uns après les autres, tant que la queue de détente reste pressée. Le rechargement s'effectue automatiquement par un mécanisme interne utilisant une part de l'énergie de la charge de chaque munition ou grâce à un moteur.

(2) Une arme semi-automatique ne tire qu'une seule munition à chaque action sur sa queue de détente mais assure seule son rechargement tant que les munitions disponibles le permettent. Une partie de l'énergie créée par le tir est utilisée pour faire fonctionner le mécanisme d'éjection de l'étui et de chargement de la cartouche suivante. Si une munition est défectueuse, l'arme est bloquée, c'est à dire enrayée.

(3) Article R. 311-2 du code de la sécurité intérieure.

professionnelle ou sportive *par des personnes, sous réserve des engagements internationaux en vigueur et des exigences de l'ordre et de la sécurité publics* [(1)]. »

La modification de cet article est l'objet du **1°** de l'article 17 du projet de loi, qui étend ces dérogations aux **tireurs sportifs** [(2)] et aux **sociétés de sécurité privée** [(3)]. Ces personnes disposent aujourd'hui d'une autorisation pour détenir des armes semi-automatiques de catégorie B, armes dont elles seraient privées dans l'exercice de leur sport ou de leur profession en l'absence de dérogation du fait du reclassement en catégorie A.

En revanche, le projet de loi écarte la possibilité offerte par la directive du 17 mai 2017 d'accorder une dérogation aux **collectionneurs**. Les articles L. 312-6-1 à L. 312-6-5 du code de la sécurité intérieure permettant de détenir au titre de la collection des armes de la seule catégorie C soumises à déclaration, et non des armes de catégorie B, rien ne justifierait qu'ils accèdent à la possession d'armes semi-automatiques au moment même du durcissement de leur régime administratif.

La rédaction initiale du projet de loi présente toutefois une **étrangeté** : elle prévoit que la dérogation s'applique pour la conduite d'activités sportives et professionnelles mais également pour les activités de collection, que l'étude d'impact jointe au projet de loi indique expressément souhaiter exclure [(4)]. Selon le rapporteur du Sénat, « *le décret en Conseil d'État prévu par l'article L. 312-2 devrait permettre d'encadrer le régime de cette dérogation, en définissant les conditions de sa mise en œuvre et en précisant la liste des personnes et entités effectivement autorisées à acquérir des armes de catégorie A* ».

L'article 17 prévoit que l'acquisition et la détention d'armes de catégorie A, à titre dérogatoire, sont soumises à un **régime d'autorisation administrative identique à celui prévu pour les armes de catégorie B**. Il procède, à cet effet, à plusieurs coordinations dans le code de la sécurité intérieure.

---

(1) Des dérogations ont ainsi été accordées aux administrations publiques pour l'équipement de leurs agents en vue de l'exercice de leurs fonctions, aux entreprises de location à des sociétés de production de films et de spectacles et aux théâtres nationaux, aux collectivités publiques et aux musées, aux entreprises se livrant à des essais industriels ainsi qu'aux experts judiciaires de la Cour de cassation ou des cours d'appel (articles R. 312-22, R. 312-26, R. 312-27, R. 312-30 et R. 312-31).

(2) Le régime applicable aux tireurs sportifs est établi aux articles R. 312-40 à R. 312-43 du code de la sécurité intérieure. Ils sont autorisés à acquérir et détenir, pour la seule pratique du tir sportif, des armes à feu de catégorie B, sous réserve de la détention d'une licence de tir en cours de validité délivrée par une fédération sportive.

(3) Les articles R. 312-37 et R. 312-38 précisent le régime applicable aux sociétés de sécurité privée. Elles peuvent acquérir et détenir des armes de catégorie B et C pour assurer la sécurité de leurs biens ou le gardiennage de leurs immeubles. Seuls leurs personnels agréés par le préfet sont autorisés à porter et utiliser ces armes. S'agissant des armes semi-automatiques qui font l'objet d'un reclassement en catégorie A, seules les entreprises de protection de navires sont actuellement concernées.

(4) « 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. »

Les utilisateurs des armes concernées demeureront donc soumis à une réglementation inchangée.

2. Deux coordinations ponctuelles

Le **7°** étend aux armes de catégorie C les règles en vigueur en matière de **vente publique d'armes** prescrites à l'article L. 312-5 du code de la sécurité intérieure, jusque-là applicables seulement aux catégories A, B et D pour partie [(1)]. Le Gouvernement considère comme une **omission** le fait que la catégorie C n'ait pas été couverte depuis l'origine.

Le ***b)*** **du 8°** procède à une coordination nécessaire à la bonne prise en compte du classement des armes neutralisées en catégorie C par le droit européen. Cette évolution est de nature réglementaire, mais elle a une incidence sur la procédure de **dessaisissement d'un détenteur d'arme** prévue à l'article L. 312-11 du code de la sécurité intérieure. Pour des raisons liées à l'ordre public ou à la sécurité des personnes, le préfet peut ordonner à tout détenteur d'armes de s'en dessaisir – soit en la vendant à un tiers autorisé à la détenir, soit en la remettant à l'État, soit en la neutralisant. Cette dernière hypothèse n'est plus envisageable dès lors que les armes neutralisées ne sont plus librement détenues, mais soumises à un régime de contrôle administratif.

3. Les modifications apportées par le Sénat

Sur proposition du rapporteur, la commission des Lois du Sénat a jugé qu'il revenait au législateur, et au non au pouvoir réglementaire, de **proscrire la détention dérogatoire d'armes de catégorie A à fin de collection**. Il a, à cet effet, modifié l'alinéa 3 de l'article 17 pour l'exclure expressément.

En outre, la commission a adopté un amendement de son rapporteur étendant à la catégorie A les dispositions de l'article L. 314-2 du code de la sécurité intérieure sur la **cession** d'armes de catégorie B entre particuliers (**11°**).

L'article 17 a été adopté **sans débat en séance publique**.

4. La position de votre Commission

Si votre commission des Lois approuve la rédaction de l'article 17 issue des travaux du Sénat, elle a toutefois adopté un amendement du rapporteur interdisant aux personnes coupables de tentative d'acquisition illégale d'armes de catégorie C de se procurer, légalement cette fois, de telles armes.

L'absence de cette incrimination en droit français constitue le seul **obstacle à la ratification** par la France du Protocole contre la fabrication et le

---

(1) Ces règles se limitent à énoncer que seules « les personnes physiques ou morales qui peuvent régulièrement acquérir et détenir des matériels et armes de ces différentes catégories *» ont la possibilité d'acheter une arme dans les ventes publiques, et que les brocantes ne peuvent en faire commerce.*

trafic illicites d'armes à feu, de leurs pièces, éléments et munitions – connu sous le nom de **Protocole des Nations unies sur les armes à feu** – adopté par résolution n° 55/255 de l'Assemblée générale de l'Organisation des nations unies du 31 mai 2001, additionnel à la Convention des Nations Unies contre la criminalité transnationale organisée. Un projet de loi d'autorisation de la ratification devrait être prochainement présenté en Conseil des ministres.

Votre rapporteur estime que l'amendement présente un **lien direct avec le projet de loi comme avec la directive transposée**, qui prévoient plusieurs dispositions répressives relatives aux conditions d'acquisition et de détention d'armes de catégorie C.

*

* *

La Commission examine les deux amendements identiques CL1 de Mme Valérie Bazin-Malgras et CL6 de M. Michel Zumkeller.

M. Jean-Louis Masson. L'amendement CL1 vise à clarifier la situation des collectionneurs en insérant, à l'alinéa 3, les mots : « ou de collection », après le mot « sportives ». On répondrait ainsi à l'inquiétude des collectionneurs et aux arguments du rapporteur, d'autant que l'amendement est conforme tout à la fois à la directive européenne et à l'avis du Conseil d'État. L'ajout proposé paraît donc raisonnable.

M. Michel Zumkeller. Cela ne coûterait pas grand-chose d'ajouter les mots « ou de collection », comme vient de l'indiquer notre collègue. Même si l'on prend en compte ce que nous a dit le rapporteur, les reconstitutions ne sont pas seules concernées : il y a également les commémorations et bien d'autres manifestations. Nous défendrons par ailleurs un amendement sur le transport puisque le rapporteur n'a pas répondu aux attentes de Jean-Luc Warsmann sur ce sujet très important.

M. le rapporteur. La question n'est pas celle, ici, de la reconstitution ou du transport des armes, mais celle du surclassement d'armes de catégorie B en catégorie A qui, de toute façon, dans l'état antérieur aux dispositions envisagées, étaient inaccessibles aux collectionneurs. En outre, dans la mesure où il s'agit de durcir la législation et non de l'assouplir, il y a aucune raison d'ouvrir aux collectionneurs la possibilité d'acquérir des armes qu'ils ne pouvaient acquérir jusqu'à présent. Avis défavorable.

M. Guillaume Larrivé. Je souhaite que le rapporteur, à la suite de ses échanges avec le Gouvernement, précise l'état des réflexions de ce dernier sur la création, ou non, d'une carte des collectionneurs. Au début de l'année 2012, nous avons fait adopter la loi du 6 mars 2012 renvoyant à un décret pour créer une carte des collectionneurs, par analogie avec ce qui existe pour les tireurs sportifs notamment. Je comprends que, pendant le mandat du président François Hollande,

ce décret n'ait pas été pris ; je comprends aussi que la question reste pendante dans les milieux concernés. Je pensais avoir déposé un amendement d'appel en ce sens mais je ne le vois pas dans la liasse électronique ; peut-être est-ce dû à une mauvaise manipulation informatique de ma part. Bref, où en est-on de la possibilité, d'ores et déjà prévue par la loi, de création d'une carte de collectionneurs ?

M. le rapporteur. Vous apportez vous-même la réponse à votre question, cher collègue : le décret n'a pas été pris. Quant à l'amendement auquel vous faites référence, je n'en ai pas eu connaissance. Mais nous sommes ici en dehors du cadre de la transposition de la directive.

M. Guillaume Larrivé. Précisément, monsieur le rapporteur, nous ne sommes pas là pour retranscrire servilement une directive – d'ailleurs je rappelle qu'une directive n'est pas un règlement –, et qu'on peut donc tout naturellement s'interroger sur les modalités de sa transposition.

Ensuite, pour nous autres législateurs, votre réponse n'est pas satisfaisante. Le décret n'a pas été pris par le Gouvernement. D'où ma question : en tant que rapporteur de la commission des Lois, l'appelez-vous à prendre ce décret ou, au contraire, pensez-vous que la carte de collectionneurs ne doit pas être créée ? Auquel cas il vous appartiendrait de présenter un amendement visant à supprimer, dans la loi du 6 mars 2012, la disposition correspondante… Bref, nous sommes bel et bien au cœur du sujet et même de l'amendement que vous venez de faire adopter relatif aux collectionneurs.

M. le rapporteur. Nous demanderons en séance publique au Gouvernement de respecter les prescriptions édictées par la loi.

M. Guillaume Larrivé. Je retiens donc que la Commission, même si nous ne votons pas sur ce point, est favorable à la création d'une carte de collectionneurs et qu'elle appelle le ministre de l'intérieur à prendre ce décret, madame la présidente.

Mme la présidente Yaël Braun-Pivet. Le rapporteur vient d'indiquer ce qu'il vient d'indiquer… La Commission en tant que telle ne s'est pas prononcée sur cette question parce qu'elle n'a pas à le faire.

M. Jean-Michel Mis. Nous pouvons féliciter M. Guillaume Larrivé d'être parvenu à poser une question sur un amendement qu'il n'a pas déposé… Notre collègue aura tout loisir d'interroger le Gouvernement sur la création éventuelle de cette carte mais il ne nous appartient pas, en tant que commissaires, de répondre en lieu et place du ministre.

*La Commission **rejette** ces amendements.*

Elle examine ensuite l'amendement CL37 du rapporteur.

M. le rapporteur. La France a signé, dans le cadre de l'Organisation des Nations unies (ONU), un protocole contre la fabrication et le trafic illicites d'armes à feu, que nous ne pouvons pas ratifier parce que notre législation ne comporte pas de référence à la tentative de se procurer illégalement des armes. Si nous introduisons cette infraction dans notre droit national, nous pourrons ratifier ce protocole et respecter nos engagements internationaux.

*La Commission **adopte** l'amendement.*

*Suivant l'avis défavorable du rapporteur, elle **rejette** les amendements identiques CL3 de Mme Valérie Bazin-Malgras et CL8 de M. Michel Zumkeller.*

Elle en vient aux amendements identiques CL2 de Mme Valérie Bazin-Malgras et CL7 de M. Michel Zumkeller.

M. Michel Zumkeller. M. Guillaume Larrivé a très bien expliqué, à propos de la création d'une carte des collectionneurs, qu'une loi a été promulguée le 6 mars 2012. Ce sera donc très bien de le rappeler en séance : à quoi bon voter des lois si les décrets d'application ne sont jamais publiés ? C'est peut-être d'ailleurs la plus belle réforme à mener : faire en sorte que les décrets d'application soient pris rapidement après la promulgation d'une loi.

Mme la présidente Yaël Braun-Pivet. De nombreuses propositions ont été faites en ce sens dans la perspective de la prochaine réforme constitutionnelle.

M. Jean-Louis Masson. L'amendement CL2 est défendu.

*Suivant l'avis défavorable du rapporteur, la Commission **rejette** ces amendements.*

Elle examine ensuite les amendements identiques CL4 de Mme Valérie Bazin-Malgras et CL21 de M. Michel Zumkeller.

M. Fabien Di Filippo. Nos collègues ne devraient pas rester insensibles à ces amendements : le retrait des armes de chasse de la catégorie D pour ne laisser au sein de cette dernière que les armes de collection est une belle opportunité. La mémoire est un devoir et de nombreux collectionneurs et restaurateurs bénévoles donnent un certain relief à nos commémorations. Il faut respecter leur travail, et leur crainte de voir les conditions de détention de ces armes et de ces véhicules devenir beaucoup plus contraignantes paraît légitime.

Mme Jacqueline Gourault, ministre auprès du ministre de l'Intérieur, avait assuré que la détention d'armes de reproduction qui ne seraient pas plus efficaces ni plus dangereuses que les armes réelles, ne serait pas plus contraignante qu'auparavant. Or le texte ne le garantit pas vraiment, hélas ! C'est pourquoi j'apporte un fervent soutien à ces deux amendements, tout comme j'étais favorable aux précédents, malheureusement rejetés. Rassurer les collectionneurs sur leur marge de manœuvre dans les années à venir serait une très bonne chose.

Suivant l'avis défavorable du rapporteur, la Commission ***rejette*** *ces amendements.*

Puis elle ***adopte*** *l'article 17* ***modifié.***

Article 18

(art. L. 313-2, L. 313-3, L. 313-5, et L. 313-6 et L. 313-7 [nouveaux] du code de la sécurité intérieure)

Encadrement de la vente d'armes, d'éléments d'armes et de munitions

Résumé du dispositif et effets principaux :

L'article 18 améliore l'encadrement des ventes d'armes, d'éléments d'armes et de munitions. Il soumet l'exercice de la profession de courtier à une procédure d'agrément préalable ; il encadre les ventes d'arme à distance ou entre particuliers pour permettre la vérification systématique de l'identité de l'acheteur ; il offre aux professionnels une base légale pour refuser de vendre une arme ou des munitions dans des conditions qu'ils jugent suspectes.

Modifications apportées par le Sénat :

Le Sénat a conditionné l'agrément d'un armurier ou d'un courtier à son honorabilité professionnelle et privée. Il a étendu le système de vérification d'identité de l'acheteur aux ventes de munitions. Enfin, il a fait mention des critères de définition d'une transaction suspecte posés par la directive du 17 mai 2017.

Modifications apportées par la commission des Lois :

La Commission a apporté au texte des modifications de nature rédactionnelle.

1. Le contrôle administratif des courtiers d'armes de catégorie C

Jusqu'à la directive du 17 mai 2017 précitée, le droit européen soumettait l'exercice de l'activité d'armurier (1) à agrément en présence d'armes de catégorie A, à simple déclaration pour la vente d'armes de catégories B et C. Les courtiers (2) n'étaient soumis à aucun contrôle.

L'article 4§3 de la directive du 18 juin 1991 modifié par la directive du 17 mai 2017 renforce le contrôle public sur le commerce des armes en soumettant à un **régime réglementaire identique** les activités d'armurier et de courtier.

---

(1) Selon l'article R. 311-1 du code de la sécurité intérieure, un armurier est une « 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) Selon le même article R. 311-1, un courtier est une « personne physique ou morale qui se livre à une activité d'intermédiation *», c'est-à-dire à des opérations à caractère commercial ou lucratif dont l'objet est de rapprocher des personnes souhaitant conclure un contrat de cession de matériels de guerre, d'armes et de munitions.*

Celui-ci impose une procédure systématique d'enregistrement, la détention d'une licence ou d'une autorisation et une vérification de l'honorabilité professionnelle et privée ainsi que des compétences professionnelles.

L'**article 18** du projet de loi transpose cette exigence européenne dans le droit national.

Le code de la sécurité intérieure édicte déjà des dispositions conformes à la directive pour la profession **d'armurier** : l'article L. 313-2 exige que le professionnel soit « *titulaire d'un agrément relatif à son honorabilité et à ses compétences professionnelles, délivré par l'autorité administrative* ». Cet agrément est délivré par le ministre de l'intérieur pour les armes de catégories A et B [(1)], par le préfet pour les catégories C et D [(2)]. 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 celle-là.

Au contraire, l'activité de **courtier** est **réglementée seulement pour les armes de catégories A ou B**. L'article L. 2332-1 du code de la défense exige ainsi une autorisation de l'État pour l'activité des intermédiaires des entreprises de fabrication et de commerce de matériels de guerre et d'armes et munitions de défense des catégories A ou B.

En conséquence, le **1° de** l'**article 18** du projet de loi modifie l'article L. 313-2 du code de la sécurité intérieure pour **étendre aux courtiers le régime applicable aux armuriers**. Un décret en Conseil d'État fixera les modalités d'application de ce nouveau régime juridique applicable aux courtiers d'armes de catégorie C. L'**article 18** aligne également la définition française de l'activité d'armurier sur celle de l'Union européenne en y intégrant les activités de modification, de location et de prêt [(3)].

2. L'encadrement des ventes d'armes à distance et entre particuliers

La directive du 17 mai 2017 renforce les obligations de **vérification de l'identité des acheteurs** d'arme en ajoutant un article 5 *ter* à la directive du 18 juin 1991. Toute transaction – y compris par correspondance, sur Internet ou à distance – donne lieu, au plus tard au moment de la livraison, au contrôle de l'identité de l'acheteur et, le cas échéant, de son autorisation d'acquisition, par l'armurier, le courtier ou l'autorité publique.

L'article L. 313-5 du code de la sécurité intérieure comporte déjà une interdiction de principe de la livraison à domicile des armes acquises par correspondance ou entre particuliers. La livraison dans les locaux d'armuriers est la règle ; toutefois, un décret en Conseil d'État peut prévoir des conditions

(1) Article R. 313-28 du code de la sécurité intérieure.

(2) Articles R. 313-1 à R. 313-7 du code de la sécurité intérieure. L'agrément est valable dix ans.

(3) Article 1er.1.9 de la directive du 18 juin 1991 modifiée par la directive du 17 mai 2017.

dérogatoires. En pratique, **le pouvoir réglementaire a renversé le principe d'interdiction** puisque l'article R. 313-23 du même code autorise les livraisons à domicile d'armes de toutes les catégories.

Ces régimes de dérogation reposent sur un contrôle de l'identité de l'acheteur qui ne fait l'objet d'aucune vérification préalable par une autorité publique ou par un armurier lorsque la transaction s'opère de particulier à particulier. Même pour les armes de catégorie B, ce contrôle n'est pas obligatoire préalablement à la transaction : l'acheteur est seulement tenu 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. **Cette situation sape l'efficacité du contrôle d'identité imposé aux armuriers et aux courtiers lors de la vente** puisque la revente peut échapper à toute supervision dès lors qu'elle s'opère à distance.

En conséquence, tant la transposition de la directive du 17 mai 2017 que le nécessaire contrôle accru des reventes d'armes imposent un durcissement des modalités de cession à distance. Le **3° de l'article 18** du projet de loi modifie l'article L. 313-5 du code de la sécurité intérieure pour que les pièces acquises par correspondance, à distance ou directement entre particuliers (1) ne puissent être livrées qu'auprès des établissements d'armuriers, aux fins de vérification de l'identité de l'acheteur, **sans possibilité de dérogation par voie réglementaire**.

L'article 18 prévoit que la transaction est « *réputée parfaite à compter de la remise effective à l'acquéreur* ». Cette précision **déroge au code civil** (2) mais permet de retenir la vente s'il s'avère que l'acheteur potentiel ne satisfait pas aux conditions légales et réglementaires pour détenir l'arme qu'il convoite. Les transactions conclues par correspondance ou à distance avec un professionnel agréé – armurier ou courtier – pourraient toujours donner lieu à livraison au domicile de l'acquéreur dans la mesure où la vérification d'identité aurait alors lieu préalablement à l'expédition de l'arme.

L'article L. 317-2 du code de la sécurité intérieure réprime la violation de ces dispositions de cinq ans d'emprisonnement et 75 000 euros d'amende.

3. Le régime des transactions suspectes

L'article 10 de la directive du 18 juin 1991 est complété par celle du 17 mai 2017 pour autoriser armuriers et courtiers à **refuser 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

---

(1) L'inclusion de la transaction directe entre particuliers n'est pas une obligation de la directive. Il s'agit d'une initiative du Gouvernement.

(2) L'article 1583 du code civil dispose que la 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 ».

que l'obligation, pour ces mêmes professionnels, de **signaler ces transactions suspectes** aux autorités compétentes.

Le **4° de l'article 18** du projet de loi transpose cette disposition en insérant dans le code de la sécurité intérieure un nouvel article L. 313-6. Il **étend aux armes** la procédure que le droit européen limitait aux seules munitions, considérant que les armuriers et les courtiers peuvent légitimement nourrir des doutes devant des demandes portant sur les unes comme sur les autres.

La possibilité de décliner la vente s'inscrit dans le cadre établi à l'article L. 121-11 du code de la consommation selon lequel « *est interdit le fait de refuser à un consommateur la vente d'un produit ou la prestation d'un service,* ***sauf motif légitime*** ». La transaction rejetée fait, par ailleurs, l'objet d'un signalement auprès de l'autorité administrative.

4. Les modifications apportées par le Sénat

La commission des Lois a adopté un amendement du rapporteur prévoyant, outre diverses améliorations rédactionnelles, la **vérification de l'identité de l'acheteur potentiel dans le cadre d'une vente de munitions** selon des modalités identiques à celles prévues au 3° pour la vente d'arme, et conditionnant l'agrément d'un armurier ou d'un courtier à son **honorabilité professionnelle comme privée**.

Quant au régime des transactions suspectes, la commission des Lois a adopté un amendement du rapporteur précisant les **critères permettant d'apprécier le caractère suspect d'une transaction –** la nature de la vente ou son échelle. Ces critères sont ceux mentionnés par la directive du 17 mai 2017.

L'article 18 n'a fait l'objet d'**aucun débat en séance publique**.

5. La position de votre Commission

La commission des Lois approuve le dispositif de l'article 18 issu des travaux du Sénat. Elle s'est bornée à adopter **six amendements rédactionnels** présentés par le rapporteur.

*

* *

La Commission ***adopte*** *successivement les amendements du rapporteur CL39 de cohérence, CL44 et CL40 rédactionnels, CL41, CL42 et CL43 rectifié, tous trois de précision.*

Puis elle ***adopte*** *l'article 18* ***modifié.***

Article 19
(art. L. 314-2-1 et L. 315-1 du code de la sécurité intérieure)
Coordinations

Résumé du dispositif et effets principaux :

L'article 19 effectue une coordination et modification de cohérence.

Modifications apportées par le Sénat :

Aucune.

Modifications apportées par la commission des Lois :

La Commission a apporté à cet article des modifications de nature rédactionnelle.

Le **I de l'article 19** effectue une coordination à l'article L. 314-2-1 du code de la sécurité intérieure à la suite de la suppression de la catégorie d'armes D1 par les précédents articles du projet de loi.

Le **II** étend aux armes de catégorie C les règles en vigueur en matière de port d'arme prescrites à l'article L. 315-1 du code de la sécurité intérieure [(1)]. Le Gouvernement considère comme une **omission** le fait que la catégorie C n'ait pas été couverte depuis l'origine.

Il a été adopté par le Sénat **sans modification**.

Votre commission des Lois approuve le dispositif de l'article 19. Elle s'est bornée à adopter **un amendement rédactionnel** du rapporteur.

*

* *

*La Commission **adopte** l'amendement rédactionnel CL45 du rapporteur.*

*Puis elle **adopte** l'article 19 **modifié**.*

Après l'article 19

La Commission examine les amendements identiques CL5 de Mme Valérie Bazin-Malgras et CL22 de M. Michel Zumkeller.

M. Jean-Louis Masson. L'amendement CL5 est défendu.

M. Michel Zumkeller. Ces deux amendements identiques concernent le transport légitime des matériels et armes historiques. C'est bien de donner le droit aux collectionneurs de participer aux commémorations avec leurs armes, mais s'ils ne peuvent pas les transporter, ce sera compliqué… Nous proposons une

(1) Ces règles consistent en l'interdiction du port d'armes de catégorie A, B et partiellement D ainsi que de leur transport sans motif légitime.

disposition grâce à laquelle ils ne seront pas dans l'illégalité entre le moment où ils partent de chez eux et celui où ils arrivent sur le lieu de la commémoration.

M. le rapporteur. Par principe, le transport des armes en France est interdit. Je reviens sur les précisions que j'ai apportées tout à l'heure sur le code de la sécurité intérieure, qui permet aux titulaires d'un permis de chasse, tout comme aux sportifs, de transporter leurs armes. J'ai de même, à l'instant, rappelé que la participation aux reconstitutions historiques est un motif légitime d'autorisation du port et du transport d'armes. Il n'y a donc pas lieu de s'inquiéter outre mesure en la matière.

M. Philippe Latombe. Je reviens sur un propos tenu au cours de la discussion générale et que j'approuve totalement : l'exposé sommaire de l'amendement CL5 contient des mots qui ne sont pas acceptables, en particulier quand il est question de « *l'abus d'autorité de la part de nombreux services des douanes, de la police ou de la gendarmerie* ». C'est assez violent. Je préfère l'exposé sommaire de l'amendement CL22 qui ne reprend pas cette expression d'« *abus d'autorité* ».

La Commission ***rejette*** *ces amendements.*

Article 20

(art. L. 317-3-1, L. 317-3-2 et L. 317-4-1 du code de la sécurité intérieure)

Coordinations

Résumé du dispositif et effets principaux :

L'article 20 effectue des coordinations à la suite de la suppression de la catégorie d'armes D1.

Modifications apportées par le Sénat :

Aucune.

Modifications apportées par la commission des Lois :

Outre des modifications de nature rédactionnelle, la Commission a complété le dispositif permettant l'adhésion de la France au Protocole des Nations unies sur les armes à feu.

L'**article 20** retire les mentions de la catégorie D des articles L. 317-3-1 et L. 317-3-2 du code de la sécurité intérieure, qui traitent des sanctions pénales encourues par un armurier ou un courtier qui manque à ses obligations légales.

Il supprime également, à l'article L. 317-4-1 du même code, l'infraction d'acquisition, de cession ou de détention prohibée d'arme de catégorie D1.

Il a été adopté par le Sénat **sans modification**.

Votre commission des Lois approuve le dispositif de l'article 20. Elle s'est bornée à adopter **deux amendements** du rapporteur :

– l'un rédactionnel ;

– l'autre, complétant les modifications apportées à l'article 17, pour permettre l'adhésion de la France au Protocole des Nations unies sur les armes à feu, en réprimant des mêmes peines l'acquisition illégale d'armes de catégorie C et sa tentative.

*

* *

*La Commission **adopte** successivement les amendements du rapporteur CL46 de précision et CL36 de cohérence.*

*Puis elle **adopte** l'article 20 **modifié**.*

Article 21

(art. L. 2331-1, L. 2339-4 et L. 2339-4-1 du code de la défense)

Coordinations dans le code de la défense

Résumé du dispositif et effets principaux :

L'article 21 procède à des coordinations au sein du code de la défense, coordinations rendues nécessaires par la suppression de la catégorie d'armes D1 par les précédents articles du titre II.

Modifications apportées par le Sénat :

Aucune.

Modifications apportées par la commission des Lois :

La Commission a apporté à cet article une modification de nature technique.

L'**article 21** supprime, aux articles L. 2331-1, L. 2339-4 et L. 2339-4-1 du code de la défense, les références aux armes de la catégorie D soumises à enregistrement que suppriment les précédents articles du titre II.

Il a été adopté par le Sénat **sans modification**.

Votre commission a dopté un **amendement de conséquence** du rapporteur, en cohérence avec le dispositif des précédents articles du projet de loi.

*

* *

*La Commission **adopte** l'amendement de conséquence CL47 du rapporteur. Puis elle **adopte** l'article 21 **modifié**.*

Article 21 bis
(art. 9 de la loi n° 55-385 du 3 avril 1955 relative à l'état d'urgence)
Coordination dans la loi relative à l'état d'urgence

Résumé du dispositif et effets principaux :

L'article 21 *bis* est issu d'un amendement du rapporteur du Sénat adopté par la commission des Lois. Il procède à une coordination au sein de la loi n° 55-385 du 3 avril 1955 relative à l'état d'urgence, coordination rendue nécessaire par la suppression de la catégorie d'armes D1 par les précédents articles du titre II.

Modifications apportées par la commission des Lois :

Aucune.

Sur proposition de son rapporteur, la commission des Lois du Sénat a inséré dans le projet de loi un **nouvel article 21 *bis*** supprimant la mention des armes de catégorie D à l'article 9 de la loi n° 55-385 du 3 avril 1955 relative à l'état d'urgence. Cette coordination est nécessaire du fait de la suppression de la catégorie d'armes D1 par les précédents articles du titre II.

L'article 21 *bis* n'a fait l'objet d'**aucun débat en séance publique au Sénat**. Il a été adopté **sans modification** par la commission des Lois de l'Assemblée nationale.

*

* *

*La Commission **adopte** l'article 21* bis ***sans modification.***

TITRE III
DISPOSITIONS RELATIVES AU SERVICE PUBLIC RÉGLEMENTÉ DE RADIONAVIGATION PAR SATELLITE

Le titre III du projet de loi se compose d'un unique article 22. Il institue un régime d'autorisation et de sanction pour le service public réglementé offert par le système mondial de radionavigation par satellite issu du programme Galileo.

À l'initiative du rapporteur, votre commission a **amendé l'intitulé de ce titre III** en faisant disparaître la mention de « Galileo » au profit d'une référence à la fonction offerte – la radionavigation par satellite. Cette modification est cohérente avec l'intitulé du chapitre que le projet de loi insère dans le code de la défense. Elle présente aussi l'avantage de ne pas inscrire dans la loi une dénomination de nature commerciale qui pourrait être amenée à évoluer à l'avenir, quand la nature des fonctionnalités offertes resteront au contraire constantes.

Avant l'article 22

*La Commission **adopte** l'amendement de cohérence CL48 du rapporteur portant sur l'intitulé du titre III.*

Article 22

(art. L. 2323-1 à 2323-6 [nouveaux] du code de la défense)

Création d'un régime d'autorisation et de sanction spécifique pour le service public réglementé (SPR) de radionavigation par satellite

Résumé du dispositif et effets principaux :

L'article 22 du projet de loi crée un régime d'autorisation et de sanction spécifique pour le service public réglementé offert par le système mondial de radionavigation par satellite issu du programme européen Galileo.

Modifications apportées par le Sénat :

Aucune.

Modifications apportées par la commission des Lois :

Aucune.

1. L'État du droit

a. Un projet européen ambitieux

Galileo est un **système de positionnement par satellites** (1) développé par l'Union européenne, incluant un segment spatial. Condition de l'indépendance stratégique de l'Europe, il est l'équivalent du GPS américain (2), du GLONASS russe (3) et du COMPASS chinois (4).

---

(1) Un système de positionnement par satellites fournit à son utilisateur ses coordonnées géographiques (longitude et latitude) et sa vitesse de déplacement. Cette information est obtenue en mesurant la distance entre le récepteur de l'utilisateur et un satellite artificiel dont la position dans l'espace est connue avec précision. En combinant la mesure simultanée de la distance d'au moins quatre satellites, le récepteur fournit la position, l'altitude et la vitesse avec une grande précision. Le récepteur peut être au sol ou embarqué dans un véhicule en déplacement.

(2) Le Global Positioning System *(GPS) (en français* Géo-positionnement par satellite*), aussi connu sous le nom de* Navstar*, est le premier système de géolocalisation fonctionnant sur l'exploitation de signaux radio émis par une constellation de satellites dédiés. Mis en place à partir de 1973 par le département de la Défense des États-Unis à des fins militaires, le système est opérationnel depuis 1995 et s'est ouvert aux applications civiles en 2000.*

(3) Conçu par l'URSS, le GLONASS ou Système global de navigation satellitaire *est opérationnel depuis 1996.*

(4) Le système Beidou *ou COMPASS est un système de navigation et de positionnement par satellites chinois en cours de déploiement. Il est pour l'heure utilisable uniquement dans la zone Asie-Pacifique, mais devrait devenir opérationnel à l'échelle mondiale en 2020.*

La Cour des comptes a évalué le coût de Galileo à **une dizaine de milliards d'euros** [(1)]. La France y contribue pour près de 20 %.

Le projet a été envisagé par la Commission européenne dès 1998 dans une communication adressée au Conseil et au Parlement européen [(2)]. Sa concrétisation a débuté en 2003 avec la mise en place de l'**entreprise commune Galileo** [(3)], la commande des premiers satellites, l'approfondissement de la coopération internationale, la confirmation de l'allocation des fréquences et la préparation des phases de déploiement et d'exploitation. L'**Agence du GNSS européen** [(4)] a repris en 2007 l'ensemble des activités de l'entreprise commune Galileo, le partenariat public-privé laissant place à une gestion directe par l'Union européenne pour une seconde phase d'installation du système [(5)]. Le programme est désormais régi par le 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.

Après les différentes séquences de conception et de test, les premiers satellites en configuration opérationnelle ont été lancés en 2014. Les premiers services de Galileo sont **opérationnels depuis 2016**. Si dix-huit des trente satellites prévus ont été lancés, la capacité opérationnelle complète est espérée pour 2020. La constellation de trente satellites devrait être en orbite en 2021.

Galileo a été conçu pour satisfaire cinq types d'exigences :

– un **service ouvert**, gratuit et accessible à tous ;

– un **service commercial** permettant le développement d'applications à des fins professionnelles ou commerciales grâce à des performances accrues et à des données d'une valeur ajoutée supérieure à celles du service ouvert ;

– une contribution au système mondial d'alerte et de localisation de radiobalise COSPAS-SARSAT [(6)] ;

– une contribution aux services de contrôle d'intégrité destinés aux utilisateurs d'applications de sauvegarde de la vie ;

---

(1) Référé de la Cour des comptes du 26 janvier 2016, La contribution de la France aux programmes européens Galileo et EGNOS, *https://www.ccomptes.fr/fr/publications/la-contribution-de-la-france-aux-programmes-europeens-galileo-et-egnos*

(2) Communication de la Commission au Conseil et au Parlement européen – Vers un réseau transeuropéen de positionnement et de navigation comprenant une stratégie européenne pour un système mondial de navigation par satellites (GNSS)/COM/98/0029 final du 21 janvier 1998.

(3) Règlement (CE) n° 876/2002 du Conseil du 21 mai 2002 créant l'entreprise commune Galileo.

(4) Créée par le règlement n° 1321/2004 du Conseil du 12 juillet 2004, son siège est à Prague.

(5) 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).

(6) À l'origine composé de deux programmes américain et soviétique, le système est désormais international et unifié. COSPAS signifie Cosmicheskaya Sistyema Poiska Avariynich Sudow *(système spatial pour la recherche des navires en détresse) et SARSAT* Search and Rescue Satellite-Aided Tracking *(localisation par satellite pour les opérations de recherche et sauvetage).*

– un **service public réglementé (SPR)**, réservé aux seuls utilisateurs autorisés par les États, pour les applications sensibles soumises à un contrôle d'accès efficace et garantissant une continuité du service dans les situations les plus graves.

b. La décision n° 1104/2011/UE du 25 octobre 2011

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, précise les **obligations des États membres** qui souhaitent recourir au **service public réglementé**. Cette décision requiert que l'accès au SPR soit restreint à certains utilisateurs sous le contrôle permanent d'une « *autorité responsable du service public réglementé* ». Pour la France, cette fonction est dévolue au secrétariat général de la défense et de la sécurité nationale (SGDSN).

La décision du 25 octobre 2011 (1) prévoit que les règles relatives à l'accès au SPR, aux récepteurs et modules associés et à l'exportation des équipements font l'objet de normes communes. **Sa mise en œuvre en droit national conditionne l'accès au service public réglementé**.

2. Les dispositions du projet de loi

Le droit français ne connaît le programme Galileo qu'à travers la loi n° 2014-548 du 28 mai 2014 autorisant l'approbation de l'accord relatif à l'hébergement et au fonctionnement du centre de sécurité Galileo, et son décret d'application n° 2014-1507 du 15 décembre 2014. Ces stipulations ne comportent aucune norme relative au service public réglementé.

La décision du 25 octobre 2011 est déjà **partiellement en application** dans la mesure où certaines de ses stipulations ont été reprises dans le règlement n° 1285/2013 du 11 décembre 2013 précité, d'effet direct en droit national. Sa complète mise en œuvre nécessite cependant un certain nombre d'évolutions législatives. Pour cette raison, l'**article 22** du projet de loi insère un nouveau chapitre III, intitulé « *Service public réglementé de radionavigation par satellite* », au sein du titre II « *Sécurité des systèmes d'information* » du livre III « *Régimes juridiques de défense d'application permanente* » de la deuxième partie « *Régimes juridiques de défense* » du code de la défense (2). Ce chapitre comporterait six articles répartis en deux sections, l'une relative aux « *Activités contrôlées* » et l'autre aux « *Sanctions pénales* » attachées à la violation des règles édictées.

---

(1) Décision complétée sur ce point par une décision déléguée de la Commission européenne du 15 septembre 2015 relative aux normes minimales communes auxquelles doivent se conformer les autorités responsables.

(2) Le Conseil d'État a estimé pertinente cette codification : « 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. » *(point n° 19 de l'avis sur le projet de loi délibéré le 14 novembre 2017).*

a. Le contrôle administratif de l'accès au service public réglementé (SPR)

La section 1 relative aux « *Activités contrôlées* » compte **trois nouveaux articles L. 2323-1 à L. 2323-3**.

Le **nouvel article L. 2323-1** édicte les principes généraux en matière d'**accès au service public réglementé**. Il transcrit en droit national les articles 3 à 7 de la décision du 25 octobre 2011 (1) dans le respect de la position commune 2008/944/PESC du Conseil du 8 décembre 2008 définissant des règles communes régissant le contrôle des exportations de technologie et d'équipements militaires. Il instaure un **régime d'autorisation** sous la responsabilité de l'autorité administrative – le secrétariat général de la défense et de la sécurité nationale. Ces autorisations, **éventuellement assorties de conditions ou de restrictions**, sont nécessaires à l'accès au SPR, au développement et à la fabrication de récepteurs ou de modules de sécurité et à l'exportation d'équipements, de technologies ou de logiciels conçus pour ce service. Elles **peuvent être abrogées, retirées, modifiées ou suspendues** en cas de manquement du titulaire aux conditions spécifiées pour assurer le respect des engagements internationaux de la France, protéger le service public réglementé et sauvegarder des intérêts essentiels d'ordre public ou de sécurité publique ; les modalités de contrôle par l'autorité administrative sont cependant absentes du projet de loi et seront définies par voie réglementaire. Le Conseil d'État a estimé que « ***ce régime d'autorisation préalable et de contrôle est justifié et nécessaire*** *compte tenu des enjeux liés à la sécurité du [SPR]* (2) ».

Le **nouvel article L. 2323-2** soumet à **déclaration** les transferts d'équipements liés au SPR vers d'autres États de l'Union européenne. Cette déclaration est adressée au secrétariat général de la défense et de la sécurité nationale. Conforme à l'article 17 de la décision déléguée de la Commission européenne du 15 septembre 2015 précitée ainsi qu'à la politique de la France en matière de transfert de produits liés à la défense vers les autres États de l'Union européenne pour la mise en œuvre d'un programme de coopération en matière d'armements dans l'Union européenne (3), le mécanisme proposé est jugé « *justifié* » par le Conseil d'État (4).

Quant au **nouvel article L. 2323-3**, il précise que les modalités d'application de la section sont établies par décret en Conseil d'État. Il indique également que les articles précédents sont mis en œuvre sans préjudice, d'une part, des dispositions du code de la défense relatives aux importations et exportations de matériels de guerre et, d'autre part, du règlement européen 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.

---

(1) Une table de correspondance entre les stipulations de la décision et les dispositions de l'article 22 figure en annexe III de l'étude d'impact jointe au projet de loi.

(2) Point n° 21 de l'avis du Conseil d'État sur le projet de loi délibéré le 14 novembre 2017.

(3) Article L. 2335-10 du code de la défense.

(4) Point n° 22 de l'avis du Conseil d'État.

Cette précaution, que le Conseil d'État a qualifiée d' « *opportune* » [1], réserve les cas dans lesquels les technologies et équipements relevant du SPR seraient également soumis à un autre régime de contrôle des exportations.

b. Les sanctions pénales attachées aux manquements

La section 2 relative aux « *Sanctions pénales* » compte **trois nouveaux articles L. 2323-4 à L. 2323-6**. Elle transcrit en droit national les stipulations de la décision du 25 octobre 2011 précitée selon laquelle les sanctions réprimant la violation de ses dispositions doivent être efficaces, proportionnées et dissuasives.

Le **nouvel article L. 2323-4** sanctionne d'une amende de 200 000 euros le fait de se livrer ou de tenter de se livrer à l'une des activités prévues à l'article L. 2323-1 sans une autorisation ou sans en respecter les modalités.

Le **nouvel article L. 2323-5** réprime d'une amende de 50 000 euros la méconnaissance de l'obligation de déclaration prévue à l'article L. 2323-2. Ce montant est inférieur à celui de l'amende prévue à l'article précédent, les enjeux stratégiques d'un transfert au sein de l'Union européenne apparaissant moindres que ceux d'une exportation vers un pays tiers.

Enfin, le **nouvel article L. 2323-6** prévoit des **peines complémentaires** pour les personnes coupables des infractions prévues aux articles précédents :

– le **I** énumère les peines complémentaires encourues par les personnes **physiques**, soit la **confiscation** « de la chose qui a servi ou était destinée à commettre l'infraction ou de la chose qui en est le produit » [2], l'**interdiction d'exercice de certaines activités** publiques ou professionnelles pour cinq ans [3], la **fermeture des établissements ayant servi à commettre les faits incriminés** [4] et l'**exclusion des marchés publics** [5].

– le **II** prévoit pour les personnes **morales** déclarées responsables pénalement, outre le quintuplement du montant maximal de l'amende à laquelle s'exposent les personnes physiques [6], les peines complémentaires suivantes : la **dissolution**, l'**interdiction d'exercice**, la **fermeture d'un établissement**, l'**exclusion des marchés publics**, la **confiscation**, la **publication** de la décision de condamnation et l'**interdiction de percevoir une aide publique**.

---

(1) Point n° 25 de l'avis du Conseil d'État.

(2) Article 131-21 du code pénal.

(3) Article 131-27 du code pénal.

(4) Article 131-33 du code pénal.

(5) Article 131-34 du code pénal.

(6) Article 131-38 du code pénal.

Ces dispositions apparaissent répondre aux principes de légalité, de nécessité et de proportionnalité des peines [(1)].

3. Les modifications apportées par le Sénat

L'article 22 a été adopté par le Sénat **sans modification**.

*

* *

*La Commission **adopte** l'article 22 **sans modification**.*

Après l'article 22

La Commission examine l'amendement CL11 de M. Ugo Bernalicis.

Mme Danièle Obono. Le présent amendement a trait à l'indépendance du système GALILEO par rapport à d'autres puissances – enjeu de gouvernance numérique à nos yeux. Le 25 octobre 2011, un article présentait GALILEO comme un service qui renverrait le GPS américain au magasin des antiquités : alors que la précision de ce dernier est de 20 mètres, celle de GALILEO sera de 4 mètres, voire 10 centimètres pour les services payants. En outre, le système européen offrira une continuité du signal inconnue du GPS ouvert au civil. Certes, la construction du programme a pris du retard, mais il nous paraît impensable que l'État puisse accepter une interopérabilité de GALILEO avec le GPS américain. Les informations manquent quant à la volonté du Gouvernement et de l'Union européenne de promouvoir ou non l'interopérabilité, au niveau mondial, des systèmes globaux de navigation par satellite. Nous souhaitons donc connaître en détail les intentions du Gouvernement.

M. le rapporteur. Je reprends à mon compte la pratique constante de la commission des Lois consistant à ne pas voter les demandes de rapport. Reste que, sur le fond, l'interopérabilité des systèmes de navigation par satellite est un sujet intéressant. Elle est déjà pratiquée avec les radiobalises. Le lieu qui me paraît toutefois le plus adapté pour discuter de la question reste l'Office parlementaire d'évaluation des choix scientifiques et technologiques (OPECST) ; c'est pourquoi je vous invite à vous rapprocher de son président, notre collègue Cédric Villani, pour lui faire part de vos préoccupations.

*La Commission **rejette** l'amendement.*

---

(1) À titre de comparaison, l'article L. 2339-2 du code de la défense punit d'un emprisonnement de sept ans et d'une amende de 100 000 euros la fabrication ou le commerce, sans autorisation, de matériels, d'armes ou de munitions. Si l'article 22 ne prévoit aucune incarcération, ses amendes sont toutefois plus importantes.

TITRE IV
DISPOSITIONS APPLICABLES À L'OUTRE–MER

Article 23

(art. L. 344-1, L. 345-1, L. 345-2-1, L. 346-1 et L. 347-1 du code de la sécurité intérieure ; art. L. 2441-1, L. 2441-3-1, L. 2451-1, L. 2451-4-1, L. 2461-1, L. 2461-4-1, L. 2471-1 et L. 2471-3-1 du code de la défense)

Application outre–mer

Résumé du dispositif et effets principaux :

Le présent article a pour objet de rendre le projet de loi applicable dans les îles Wallis et Futuna, en Polynésie française, en Nouvelle-Calédonie et dans les Terres australes et antarctiques françaises, collectivités ultramarines sur le territoire desquelles une mention expresse d'application est nécessaire.

Modifications apportées au Sénat :

Le Sénat a introduit un « *compteur outre-mer* » pour l'application du titre I^er^ du projet de loi et a procédé à différentes améliorations rédactionnelles. Il a par ailleurs mis à jour le « *compteur outre-mer* » de la loi n° 55-385 du 3 avril 1955 relative à l'état d'urgence.

1. Le dispositif proposé

Le **I du présent article** dispose que les dispositions du titre V du projet de loi, qui ne font l'objet d'aucune codification, seront applicables sur l'ensemble du territoire de la République.

L'article 2 du projet de loi comporte une référence au règlement européen (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, qui n'est pas applicable aux îles Wallis et Futuna, en Polynésie française, en Nouvelle-Calédonie et dans les Terres australes et antarctiques françaises. En conséquence, le **deuxième alinéa du présent article** précise expressément que sera applicable, dans ces mêmes territoires, le droit applicable en métropole en vertu de ce règlement.

Le **II du présent article** est relatif à l'application du titre II du projet de loi, qui modifie des dispositions codifiées au sein du code de la sécurité intérieure.

L'**alinéa 4** vise à actualiser le « *compteur outre–mer* » [(1)] des collectivités des îles Wallis et Futuna, de Polynésie française, de la Nouvelle-Calédonie et des

(1) Cette technique du compteur consiste à indiquer qu'une disposition est applicable dans une collectivité régie par le principe de spécialité législative dans sa rédaction résultant d'une loi déterminée, ce qui permet de savoir si les modifications ultérieures de cette disposition ont été ou non étendues.

Terres australes et antarctiques françaises du code de la sécurité intérieure pour prendre en compte les modifications effectuées par les articles 16 à 20 du projet de loi au livre III du code de la sécurité intérieure.

L'**alinéa 5** tire les conséquences de la suppression de la catégorie D s'agissant de la Nouvelle–Calédonie.

Le **III du présent article** est relatif à l'application du titre II du projet de loi, qui modifie des dispositions codifiées au sein du code de la défense.

Les **alinéas 7 à 10** visent à actualiser le « *compteur outre–mer* » des collectivités des îles Wallis et Futuna, de Polynésie française, de la Nouvelle-Calédonie et des Terres australes et antarctiques françaises pour prendre en compte les modifications effectuées par l'article 20 du projet de loi au livre III de la deuxième partie du code de la défense.

Les **alinéas 11 à 13** disposent que seront applicable, à Wallis–et–Futuna, le droit en vigueur en métropole en vertu 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 **alinéas 14 à 16** procèdent à la même précision s'agissant de la Polynésie française.

Les **alinéas 17 à 19** procèdent à la même précision s'agissant de la Nouvelle–Calédonie.

Les **alinéas 20 à 22** procèdent à la même précision s'agissant des Terres australes et antarctiques françaises.

Seuls les articles L. 2323-2 et L. 2323-5 du code de la défense, créés par l'article 22 du projet de loi, ne seraient pas applicables aux territoires ultra-marins, dans la mesure où ils concernent les transferts intracommunautaires, qui ne leur sont pas applicables.

2. Les modifications apportées par le Sénat

À l'initiative de son rapporteur, la commission des Lois a adopté un amendement introduisant un « *compteur outre-mer* » pour l'application du titre I^{er} du projet de loi.

Elle a également procédé à différentes améliorations rédactionnelles et mis à jour le « *compteur outre-mer* » de la loi n° 55-385 du 3 avril 1955 relative à l'état d'urgence afin d'assurer l'application en outre-mer des modifications introduites par l'article 21 *bis*.

*

* *

*La Commission **adopte** successivement les amendements rédactionnels CL27 et CL49 du rapporteur.*

*Puis elle **adopte** l'article 23 **modifié**.*

TITRE V
DISPOSITIONS TRANSITOIRES

Article 24
Dispositions transitoires

Résumé du dispositif et effets principaux :

Le présent article a pour objet de reporter l'entrée en vigueur de certaines dispositions du projet de loi.

Modifications apportées au Sénat :

Le Sénat a adopté un amendement précisant que les dispositions de l'ensemble du titre I[er] entreraient en vigueur au plus tard le 9 mai 2018.

1. Le dispositif proposé

Le **premier alinéa du présent article** prévoit que l'entrée en vigueur du titre I[er], à l'exception du chapitre II relatif aux opérateurs de services essentiels (OSE), est fixée à une date déterminée par décret en Conseil d'État et devrait intervenir au plus tard le 9 mai 2018, soit la date maximale de transposition de la directive. Il précise par ailleurs, conformément à la directive (UE) 2016/1148 précitée du 6 juillet 2016, dite directive « *NIS* », que la désignation des OSE interviendrait au plus tard le 9 novembre 2018.

La commission des Lois du Sénat, à l'initiative de son rapporteur, a adopté un amendement précisant que les dispositions de l'ensemble du titre I[er] entreraient en vigueur au plus tard le 9 mai 2018, seule la désignation des OSE pouvant intervenir ultérieurement.

Les **alinéas 2, 3 et 4 du présent article** sont relatifs à l'entrée en vigueur du titre II du présent projet de loi, transposant la directive (UE) 2017/853 du 17 mai 2017 relative à l'acquisition et à la détention d'armes. Cette entrée en vigueur est également renvoyée à une date fixée par décret en Conseil d'État et au plus tard le 14 septembre 2018, date maximale fixée par la directive, à l'exception des dispositions du 1° de l'article 18 relatives à l'instauration d'un contrôle administratif à l'égard des courtiers qui entreront en vigueur au plus tard le 14 décembre 2019, comme prévu par la directive (**alinéa 3 du présent article**).

Le **quatrième alinéa du présent article** fixe le régime transitoire applicable aux détenteurs d'armes de catégorie D1 acquises après la date d'entrée en vigueur de la directive, c'est-à-dire depuis le 13 juin 2017. Comme précisé dans le cadre du commentaire de l'article16, ces détenteurs auraient une obligation de régulariser leur situation et de procéder à la déclaration de leur arme auprès du préfet, dans des conditions fixées par décret en Conseil d'État.

*

* *

*La Commission **adopte** l'amendement de précision rédactionnelle CL28 du rapporteur.*

*Puis elle **adopte** l'article 24 **modifié**.*

*Enfin, la Commission **adopte** l'ensemble du projet de loi **modifié**.*

*

* *

*En conséquence, la commission des Lois constitutionnelles, de la législation et de l'administration générale de la République vous demande **d'adopter** le projet de loi (n° 530) portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité dans le texte figurant dans le document annexé au présent rapport.*

LISTE DES PERSONNES ENTENDUES

MINISTÈRES ET ADMINISTRATIONS

- **Ministère de l'Intérieur – Cabinet**

  — M. Julien Autret, conseiller parlementaire

- **Secrétariat d'État chargé du Numérique**

  — M. Côme Berbain, conseiller transformation numérique de l'État et sécurité numérique

- **Service central des armes du ministère de l'Intérieur**

  — M. Pascal Girault, chef de service

- **Agence nationale de la sécurité des systèmes d'information (ANSSI)**

  — M. Guillaume Poupard, directeur général

  — M. Julien Barnu, directeur de cabinet

  — M. Denys Legrand, chargé de mission à la sous-direction relations extérieures et coordination

  — Mme Marie Prévot, conseillère juridique du secrétaire général de la défense et de la sécurité nationale

  — M. Gwénaël Jezequel, conseiller relations institutionnelles et communication du secrétaire général de la défense et de la sécurité nationale

ORGANISATION

- **Fédération des Industries Electriques, Electroniques et de Communication**

  — M. Guillaume Adam, chef de service Affaires européennes et numériques

  — M. Yoann Kassianides, délégué général

  — M. Pencho Stanchev, business développement, France Operations

ANNEXE : TABLEAU COMPARATIF DU TITRE I^ER DU PROJET DE LOI ET DE LA DIRECTIVE « NIS »

Projet de loi	Directive « *NIS* »
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 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. 4** 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 ; 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 (…).
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.	**Art. 1er** (…) 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) n° 910/2014. (…) Lorsqu'un acte juridique sectoriel de l'Union exige des opérateurs de services

[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.	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. 3 « 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. » 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, 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 numérique.
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. 14, 5** 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 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.
Article 4 (décret)	

Art. 5, al. 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.	**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, al. 1 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, 3** Aux fins du paragraphe 1, chaque État membre établit une liste des services visés au paragraphe 2, point a).
Art. 5, al. 1 « [...] La liste de ces opérateurs est actualisée à intervalles réguliers et au moins tous les deux ans. »	**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, 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. 3** 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. 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	**Art. 14, 1 et 2** 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

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. »	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 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.	**Art. 14, 3 et 4** 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. 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. 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. 8 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. 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	**Art. 15, 1 et 2** 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 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 oeuvre effective des politiques de sécurité, tels que les résultats d'un audit de sécurité exécuté par l'autorité

afin d'effectuer des analyses et des relevés d'informations techniques.	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.
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.	**Art. 15, 3** 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. 9. 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. 21.** 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. 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 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. 4** Aux fins de la présente directive, on entend par : (…) 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 dont le type figure dans la liste de l'annexe III; 6) « fournisseur de service numérique » : une personne morale qui fournit un service numérique; (…) 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 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.
Art. 11 Sont soumis aux dispositions du présent chapitre les fournisseurs de service numérique offrant leurs services dans l'Union européenne et dont le siège	**Art. 18, 1 et 2** 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

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.	son établissement principal. Un fournisseur de service numérique est réputé 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.
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. »	**Art. 16, 11** 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. 12 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.	**Art. 16, 1 et 2** 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.
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 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.	**Art. 16, 3 et 4** 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 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.
Art. 13, al.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	**Art. 16, 6** 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,

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.	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.
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 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.	**Art. 17, 1 et 2** 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. 15 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	**Art. 21** 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

mentionnées dans une mise en demeure, à l'expiration du délai défini par celle-ci. 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.	appliquées. Les sanctions prévues sont effectives, proportionnées et dissuasives.