N° 7314

CHAMBRE DES DEPUTES

Session ordinaire 2017-2018

P R O J E T D E L O I

portant transposition de la directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union et modifiant

1. **la loi du 23 juillet 2016 portant création d'un Haut-Commissariat à la Protection nationale et**
2. **la loi modifiée du 20 avril 2009 portant création du Centre des technologies de l'information de l'Etat**

* * *

(Dépôt: le 6.6.2018)

SOMMAIRE:

*

ARRETE GRAND-DUCAL DE DEPOT

Nous HENRI, Grand-Duc de Luxembourg, Duc de Nassau,

Sur le rapport de Notre Premier ministre, ministre d'Etat et après délibération du Gouvernement en Conseil ;

Arrêtons :

Article unique.– Notre Premier ministre, ministre d'Etat est autorisé à déposer en Notre nom à la Chambre des Députés le projet de loi portant transposition de la directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union et modifiant

1. la loi du 23 juillet 2016 portant création d'un Haut-Commissariat à la Protection nationale et
2. la loi modifiée du 20 avril 2009 portant création du Centre des technologies de l'information de l'Etat.

Château de Berg, le 9 mai 2018

Le Premier ministre,
ministre d'Etat,
Xavier BETTEL

HENRI

*

TEXTE DU PROJET DE LOI

Chapitre 1er – *Définitions et champ d'application*

Art. 1er. Pour l'application de la présente loi, on entend par :

1. « Réseau et système d'information » :
   a) un réseau de communications électroniques au sens de l'article 2, paragraphe 24, de la loi modifiée du 27 février 2011 sur les réseaux et les services de communications électroniques ;
   b) tout dispositif ou tout ensemble de dispositifs interconnectés ou apparentés, dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement automatisé de données numériques ; ou
   c) les données numériques stockées, traitées, récupérées ou transmises par les éléments visés aux points a) et b) en vue de leur fonctionnement, utilisation, protection et maintenance ;
2. « Sécurité des réseaux et des systèmes d'information » : la capacité des réseaux et des systèmes d'information de résister, à un niveau de confiance donné, à des actions qui compromettent la disponibilité, l'authenticité, l'intégrité ou la confidentialité de données stockées, transmises ou faisant l'objet d'un traitement, et des services connexes que ces réseaux et systèmes d'information offrent ou rendent accessibles ;
3. « Opérateur de services essentiels » : une entité publique ou privée ayant un établissement sur le territoire luxembourgeois dont le type figure en annexe et qui répond aux critères énoncés à l'article 6, paragraphe 1er ;
4. « Service numérique » : un service au sens de l'article 1er, paragraphe 1er, point b), de la loi du 8 novembre 2016 prévoyant une procédure d'information dans le domaine des réglementations techniques et des règles relatives aux services de la société de l'information du type « place de marché en ligne », « moteur de recherche en ligne » ou « service d'informatique en nuage » ;
5. « Fournisseur de service numérique » : une personne morale qui fournit un service numérique ;
6. « Incident » : tout événement ayant un impact négatif réel sur la sécurité des réseaux et des systèmes d'information;

7. « Gestion d'incident » : toutes les procédures utiles à la détection, à l'analyse et au confinement d'un incident et toutes les procédures utiles à l'intervention en cas d'incident ;
8. « Risque » : toute circonstance ou tout événement raisonnablement identifiable ayant un impact négatif potentiel sur la sécurité des réseaux et des systèmes d'information ;
9. « Représentant » : une personne physique ou morale établie dans l'Union qui est expressément désignée pour agir pour le compte d'un fournisseur de service numérique non établi dans l'Union ;
10. « Norme » : une norme au sens de l'article 2, point 1), du règlement (UE) n° 1025/2012 ;
11. « Spécification » : une spécification technique au sens de l'article 2, point 4), du règlement (UE) n° 1025/2012 ;
12. « Point d'échange internet » (IXP) : une structure de réseau qui permet l'interconnexion de plus de deux systèmes autonomes indépendants, essentiellement aux fins de faciliter l'échange de trafic internet ; un IXP n'assure l'interconnexion que pour des systèmes autonomes ; un IXP n'exige pas que le trafic internet passant entre une paire quelconque de systèmes autonomes participants transite par un système autonome tiers, pas plus qu'il ne modifie ou n'altère par ailleurs un tel trafic ;
13. « Système de noms de domaine » (DNS) : un système hiérarchique et distribué d'affectation de noms dans un réseau qui résout les questions liées aux noms de domaines ;
14. « Fournisseur de services DNS » : une entité qui fournit des services DNS sur l'internet ;
15. « Registre de noms de domaine de haut niveau » : une entité qui administre et gère l'enregistrement de noms de domaine internet dans un domaine de haut niveau donné ;
16. « Place de marché en ligne » : un service numérique qui permet à des consommateurs et/ou à des professionnels au sens de l'article L. 010-1, point 1) ou point 2) respectivement, 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 ;
17. « 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 ;
18. « Service informatique en nuage » : un service numérique qui permet l'accès à un ensemble modulable et variable de ressources informatiques pouvant être partagées ;
19. « Autorité compétente concernée » : la Commission de surveillance du secteur financier (ci-après « la CSSF ») est l'autorité compétente en matière de sécurité des réseaux et des systèmes d'information couvrant les secteurs des banques et des infrastructures de marchés financiers tels que définis aux points 3. et 4. de l'annexe, ainsi que les services numériques fournis par une entité tombant sous la surveillance de la CSSF. L'Institut luxembourgeois de régulation (ci-après « l'ILR ») est l'autorité compétente en matière de sécurité des réseaux et des systèmes d'information couvrant les autres secteurs visés en annexe, ainsi que les services numériques fournis par une entité pour laquelle la CSSF n'est pas l'autorité compétente ;
20. « Point de contact national unique » : l'ILR constitue le point de contact national unique en matière de sécurité des réseaux et des systèmes d'information ;
21. « CERT Gouvernemental » : Centre de traitement des urgences informatiques, tel que défini à l'arrêté grand-ducal du xx.xx.xx déterminant l'organisation et les attributions du Centre de traitement des urgences informatiques, dénommé « CERT Gouvernemental » ;
22. « CIRCL » : Computer Incident Response Center Luxembourg, opéré par le G.I.E. Security Made in Lëtzebuerg ;
23. « CSIRT » : centre de réponse aux incidents de sécurité informatiques ;
24. « Groupe de coopération » : groupe institué aux fins de soutenir et de faciliter la coopération stratégique et l'échange d'informations entre les Etats membres et de renforcer la confiance, et de parvenir à un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union ;
25. « Réseau des CSIRT » : groupe institué aux fins de contribuer au renforcement de la confiance entre les Etats membres et de promouvoir une coopération opérationnelle rapide et effective.

Art. 2 (1) Les exigences en matière de sécurité et de notification prévues par la présente loi ne s'appliquent pas aux entreprises soumises aux exigences énoncées aux articles 45 et 46 de la loi modifiée du 27 février 2011 sur les réseaux et les services de communications électroniques ni aux prestataires de services de confiance soumis aux exigences à l'article 19 du règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE.

(2) Lorsqu'une loi ou un acte juridique sectoriel de l'Union exige des opérateurs de services essentiels ou des fournisseurs de service numérique qu'ils assurent la sécurité de leurs réseaux et systèmes d'information ou qu'ils procèdent à la notification des incidents, à condition que les exigences en question aient un effet au moins équivalent à celui des obligations prévues par la présente loi, les dispositions de cette loi ou de cet acte juridique sectoriel de l'Union s'appliquent.

Chapitre 2 – *Autorités compétentes concernées et point de contact national unique*

Art. 3. Dans la limite de leurs compétences et missions, les autorités compétentes concernées ont le pouvoir de prendre des règlements dans le cadre de l'exécution de la présente loi.

Art. 4. Dans l'exercice de sa mission, l'ILR bénéficie d'une contribution financière à charge du budget de l'Etat, à titre de participation aux frais de fonctionnement.

Art. 5. Le point de contact unique exerce une fonction de liaison pour assurer une coopération transfrontalière entre les autorités des Etats membres, ainsi qu'avec les autorités concernées des autres Etats membres, le groupe de coopération et le réseau des CSIRT.

Chapitre 3 – *Opérateurs de services essentiels*

Art. 6. (1) L'identification des opérateurs de services essentiels par l'autorité compétente concernée se fait au moyen des critères d'identification suivants :

1. une entité fournit un service qui est essentiel au maintien d'activités sociétales et/ou économiques critiques ;
2. la fourniture de ce service est tributaire des réseaux et des systèmes d'information ; et
3. un incident aurait un effet disruptif important sur la fourniture dudit service.

L'autorité compétente concernée notifie la décision d'identification à l'opérateur de services essentiels.

(2) L'importance de l'effet disruptif visé au paragraphe 1er, point 3., est déterminée sur base de facteurs transsectoriels et sectoriels, dont notamment :

1. le nombre d'utilisateurs tributaires du service fourni par l'entité concernée ;
2. la dépendance des autres secteurs visés en annexe à l'égard du service fourni par cette entité ;
3. les conséquences que des incidents pourraient avoir, en termes de degré et de durée, sur les fonctions économiques ou sociétales ou sur la sûreté publique ;
4. la part de marché de cette entité ;
5. la portée géographique eu égard à la zone susceptible d'être touchée par un incident ;
6. l'importance que revêt l'entité pour garantir un niveau de service suffisant, compte tenu de la disponibilité de solutions de rechange pour la fourniture de ce service.

(3) La liste des services essentiels est fixée par l'autorité compétente concernée.

(4) Lorsqu'une entité fournit un service visé au paragraphe 1er, point 1., dans un autre Etat membre, l'autorité compétente concernée se consulte avec l'autorité compétente de l'autre Etat membre. La consultation intervient avant que l'identification ne fasse l'objet d'une décision.

Art. 7. (1) 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. Afin d'identifier les risques, les opérateurs de services essentiels utilisent un cadre d'analyse de risques approprié pouvant être précisé par l'autorité compétente concernée.

(2) Les opérateurs de services essentiels prennent des 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.

(3) Les mesures prises sur base des paragraphes 1 et 2 sont notifiées à l'autorité compétente concernée. Les modalités de cette notification et notamment le format et le délai, sont déterminées par l'autorité compétente concernée.

(4) Les opérateurs de services essentiels notifient à l'autorité compétente concernée, sans retard injustifié, les incidents qui ont un impact significatif sur la continuité des services essentiels qu'ils fournissent. Ces notifications sont transmises au CERT Gouvernemental et au CIRCL en fonction de leurs compétences respectives. Les notifications contiennent des informations permettant à l'autorité compétente concernée de déterminer si l'incident a un impact au niveau transfrontalier. Cette notification n'accroît pas la responsabilité de la partie qui en est à l'origine.

(5) L'ampleur de l'impact d'un incident est déterminée en tenant compte des paramètres suivants :

1. le nombre d'utilisateurs touchés par la perturbation du service essentiel ;
2. la durée de l'incident ;
3. la portée géographique eu égard à la zone touchée par l'incident.

L'autorité compétente concernée peut préciser les modalités et délais des notifications des incidents qui ont un impact significatif sur la continuité des services essentiels qu'ils fournissent.

(6) Sur la base des informations fournies dans la notification de l'opérateur de services essentiels, l'autorité compétente concernée signale aux autres Etats membres touchés si l'incident est susceptible d'avoir un impact significatif sur la continuité des services essentiels dans ces Etats membres. Ce faisant, l'autorité compétente concernée 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.

Lorsque les circonstances le permettent, l'autorité compétente concernée fournit à l'opérateur de services essentiels qui est à l'origine de la notification des informations utiles au suivi de sa notification.

À la demande de l'autorité compétente concernée, le point de contact national transmet les notifications visées au premier alinéa aux points de contact nationaux des autres Etats membres touchés.

(7) Une fois par an, l'autorité compétente concernée transmet au point de contact unique 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 aux paragraphes (4) et (6).

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 aux paragraphes (4) et (6).

(8) Après avoir consulté l'opérateur de services essentiels qui est à l'origine de la notification, l'autorité compétente concernée peut informer le public d'incidents particuliers ou imposer à l'opérateur de services essentiels de le faire, lorsque la sensibilisation du public est nécessaire pour prévenir un incident ou gérer un incident en cours, ou lorsque la divulgation de l'incident est dans l'intérêt public à d'autres égards.

Art. 8. (1) A la demande de l'autorité compétente concernée, les opérateurs de services essentiels lui fournissent :

1. les informations nécessaires pour évaluer la sécurité de leurs réseaux et systèmes d'information, y compris les documents relatifs à leurs politiques de sécurité ;
2. des éléments prouvant la mise en œuvre effective des politiques de sécurité, tels que les résultats d'un audit de sécurité exécuté par l'autorité compétente concernée 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 concernée. L'autorité compétente concernée peut charger un auditeur externe de contrôler la mise en œuvre effective de la politique de sécurité à charge de l'opérateur de services essentiels ;
3. toute information nécessaire à l'accomplissement de ses missions en vertu de la présente loi.

Les opérateurs de services essentiels fournissent ces informations en respectant les délais et le niveau de détail exigés par l'autorité compétente concernée.

Au moment de formuler une telle demande d'informations et de preuves, l'autorité compétente concernée mentionne la finalité de la demande et précise quelles sont les informations exigées.

(2) Après évaluation des informations ou des résultats des audits de sécurité visés au paragraphe 1er, l'autorité compétente concernée peut donner des instructions contraignantes aux opérateurs de services essentiels pour remédier aux défaillances identifiées.

(3) Pour traiter des incidents notifiés donnant lieu à des violations des données à caractère personnel, l'autorité compétente concernée coopère étroitement avec la Commission nationale pour la protection des données et lui transmet les informations en relation avec cette violation.

Chapitre 4 – *Fournisseurs de service numérique*

Art. 9. (1) Tombent sous le champ d'application de la présente loi, les fournisseurs de service numérique ayant leur établissement principal au Grand-Duché de Luxembourg. Un fournisseur de service numérique est réputé avoir son établissement principal au Grand-Duché de Luxembourg lorsque son siège social se trouve au Grand-Duché de Luxembourg. Le fournisseur de service numérique qui n'est pas établi dans l'Union mais qui fournit un service numérique sur le territoire du Grand-Duché de Luxembourg et qui désigne un représentant au Grand-Duché de Luxembourg, relève de la compétence des autorités luxembourgeoises.

Le représentant peut être contacté par l'autorité compétente concernée à la place du fournisseur de service numérique concernant les obligations incombant audit fournisseur de service numérique en vertu de la présente loi.

La désignation d'un représentant par le fournisseur de service numérique est sans préjudice d'actions en justice qui pourraient être intentées contre le fournisseur de service numérique lui-même.

(2) Le chapitre 4 ne s'applique pas aux microentreprises et petites entreprises telles que définies dans le règlement grand-ducal du 16 mars 2005 portant adaptation de la définition des micro, petites et moyennes entreprises.

Art. 10. (1) 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, un service numérique 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 :

1. la sécurité des systèmes et des installations ;
2. la gestion des incidents ;
3. la gestion de la continuité des activités ;
4. le suivi, l'audit et le contrôle ;
5. le respect des normes internationales.

La gestion des risques qui menacent la sécurité des réseaux et des systèmes d'information des fournisseurs de service numérique se fait conformément au règlement d'exécution (UE) 2018/151 de la Commission du 30 janvier 2018 portant modalités d'application de la directive (UE) 2016/1148 du Parlement européen et du Conseil précisant les éléments à prendre en considération par les fournisseurs de service numérique pour gérer les risques qui menacent la sécurité des réseaux et des systèmes d'information ainsi que les paramètres permettant de déterminer si un incident a un impact significatif.

(2) 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 numériques qui sont offerts dans l'Union, de manière à garantir la continuité de ces services.

(3) Les fournisseurs de service numérique notifient à l'autorité compétente concernée, sans retard injustifié, tout incident ayant un impact significatif sur la fourniture d'un service numérique qu'ils offrent dans l'Union. Ces notifications sont transmises au CERT Gouvernemental et au CIRCL en fonction de leurs compétences respectives. Les notifications contiennent des informations permettant à l'autorité compétente concernée d'évaluer l'ampleur de l'éventuel impact au niveau transfrontalier. Cette notification n'accroît pas la responsabilité de la partie qui en est à l'origine.

(4) L'importance de l'impact d'un incident est déterminée en tenant compte des paramètres suivants :

1. le nombre d'utilisateurs touchés par l'incident, en particulier ceux qui recourent au service pour la fourniture de leurs propres services ;
2. la durée de l'incident ;
3. la portée géographique eu égard à la zone touchée par l'incident ;
4. la gravité de la perturbation du fonctionnement du service ;
5. 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.

Les paramètres permettant de déterminer si un incident a un impact significatif sont précisés par le règlement d'exécution (UE) 2018/151 de la Commission du 30 janvier 2018 portant modalités d'application de la directive (UE) 2016/1148 du Parlement européen et du Conseil précisant les éléments à prendre en considération par les fournisseurs de service numérique pour gérer les risques qui menacent la sécurité des réseaux et des systèmes d'information ainsi que les paramètres permettant de déterminer si un incident a un impact significatif.

(5) Lorsqu'un opérateur de services essentiels s'appuie sur un tiers fournisseur de service numérique pour la prestation d'un service essentiel au maintien de fonctions sociétales et économiques critiques, tout impact significatif sur la continuité des services essentiels en raison d'un incident touchant le fournisseur de service numérique est notifié par ledit opérateur.

(6) Lorsque l'incident visé au paragraphe 3 concerne deux Etats membres ou plus, l'autorité compétente concernée peut informer les autres Etats membres touchés. Ce faisant, l'autorité compétente concernée 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 du fournisseur de service numérique ainsi que la confidentialité des informations communiquées.

(7) Une fois par an, l'autorité compétente concernée transmet au point de contact unique 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 aux paragraphes (3) et (6).

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 aux paragraphes (3) et (6).

(8) Après avoir consulté le fournisseur de service numérique concerné, l'autorité compétente concernée, et les autorités ou les CSIRT des autres Etats membres concernés peuvent informer le public d'incidents particuliers ou imposer au fournisseur de service numérique de le faire, dans le cas où la sensibilisation du public est nécessaire pour prévenir un incident ou pour gérer un incident en cours, ou lorsque la divulgation de l'incident est dans l'intérêt public à d'autres égards.

Art. 11. (1) L'autorité compétente concernée peut imposer aux fournisseurs de service numérique :

1. de lui 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 ;
2. de corriger tout manquement aux obligations fixées à l'article 10 ;
3. de lui communiquer toute information nécessaire à l'accomplissement de ses missions en vertu de la présente loi.

(2) Si un fournisseur de service numérique a son établissement principal ou un représentant au Grand-Duché de Luxembourg alors que ses réseaux et systèmes d'information sont situés dans un ou plusieurs autres Etats membres, l'autorité compétente concernée luxembourgeoise coopère avec l'autorité compétente de ces autres Etats membres.

Chapitre 5 – *Notification volontaire*

Art. 12. (1) Les entités qui n'ont pas été identifiées en tant qu'opérateurs de services essentiels et qui ne sont pas des fournisseurs de service numérique peuvent notifier, à titre volontaire, les incidents ayant un impact significatif sur la continuité des services qu'elles fournissent.

(2) Lorsqu'elle traite des notifications, l'autorité compétente concernée agit conformément à la procédure énoncée à l'article 7. L'autorité compétente concernée peut traiter les notifications obligatoires en leur donnant la priorité par rapport aux notifications volontaires. Les notifications volontaires ne sont traitées que lorsque leur traitement ne fait pas peser de charge disproportionnée ou inutile sur l'autorités compétente concernée.

Une notification volontaire n'a pas pour effet d'imposer à l'entité qui est à l'origine de la notification des obligations auxquelles elle n'aurait pas été soumise en vertu de la présente loi si elle n'avait pas procédé à ladite notification.

Chapitre 6 – *Sanctions*

Art. 13. (1) Lorsque l'autorité compétente concernée constate une violation des obligations prévues par les articles 7, 8, 10 et 11 ou par des mesures prises en exécution de cette loi, elle peut frapper l'opérateur de services essentiels ou le fournisseur de service numérique concerné d'une ou de plusieurs des sanctions suivantes :

1. un avertissement ;
2. un blâme ;
3. une amende d'ordre, dont le montant est proportionné à la gravité du manquement, à la situation de l'intéressé, à l'ampleur du dommage et aux avantages qui en sont tirés sans pouvoir excéder 125.000 euros.

L'amende ne peut être prononcée que pour autant que les manquements visés ne fassent pas l'objet d'une sanction pénale.

Les sanctions sont effectives, proportionnées et dissuasives.

(2) En cas de constatation d'un fait susceptible de constituer un manquement visé au paragraphe 1er, l'autorité compétente concernée engage une procédure contradictoire dans laquelle l'opérateur de services essentiels ou le fournisseur de service numérique concerné a la possibilité de consulter le dossier et de présenter ses observations écrites ou verbales. L'opérateur de services essentiels ou le fournisseur de service numérique concerné peut se faire assister ou représenter par une personne de son choix. A l'issue de la procédure contradictoire, l'autorité compétente concernée peut prononcer à l'encontre de l'opérateur de services essentiels ou du fournisseur de service numérique concerné une ou plusieurs des sanctions visées au paragraphe 1er.

(3) Les décisions prises par l'autorité compétente concernée à l'issue de la procédure contradictoire sont motivées et notifiées à l'opérateur de services essentiels ou au fournisseur de service numérique concerné.

(4) Contre les décisions visées au paragraphe 3 un recours en réformation est ouvert devant le tribunal administratif.

(5) La perception des amendes d'ordre prononcées par l'ILR est confiée à l'Administration de l'Enregistrement et des Domaines.

Chapitre 7 – *Dispositions modificatives*

Art. 14. A l'article 2, point y), de loi modifiée du 20 avril 2009 portant création du Centre des technologies de l'information de l'Etat, le point final est remplacé par un point-virgule et l'article 2 de la même loi est complété comme suit :

« z) l'exercice, dans le cadre de ces attributions, de la fonction d'Autorité d'agrément cryptographique, chargée de veiller à ce que les produits cryptographiques soient conformes aux politiques de sécurité respectives en matière cryptographique; d'évaluer et d'agréer les produits cryptographiques pour la protection des informations classifiées jusqu'à un certain niveau de classification dans leur environnement opérationnel; de conserver et de gérer les données techniques relatives aux produits cryptographiques. »

Art. 15. (1) A l'article 2, point 4., de loi du 23 juillet 2016 portant création d'un Haut-Commissariat à la Protection nationale, le point final est remplacé par un point-virgule et l'article 2 de la même loi est complété comme suit :

« 5. «stratégie nationale en matière de sécurité des réseaux et des systèmes d'information»: un cadre prévoyant des objectifs et priorités stratégiques en matière de sécurité des réseaux et des systèmes d'information au niveau national. »

(2) A l'article 3, paragraphe 1er, lettre b, de la même loi, il est ajouté un point 4., rédigé comme suit :

« de coordonner et d'élaborer une stratégie nationale en matière de sécurité des réseaux et des systèmes d'information; »

(3) Dans l'article 8, paragraphe 1er, de la loi du 23 juillet 2016 portant création d'un Haut-Commissariat à la Protection nationale, les mots « l'article 5 » sont remplacés par ceux de « l'article 4 ».

(4) Dans la même loi, il est inséré un chapitre 4bis libellé comme suit :

« Chapitre 4bis – *La stratégie nationale en matière de sécurité des réseaux et des systèmes d'information*

Art. 9bis. Le Haut-Commissariat à la Protection nationale élabore une stratégie nationale en matière de sécurité des réseaux et des systèmes d'information, qui porte, en particulier, sur les points suivants :

a) les objectifs et les priorités de la stratégie nationale en matière de sécurité des réseaux et des systèmes d'information ;

b) un cadre de gouvernance permettant d'atteindre les objectifs et les priorités de la stratégie nationale en matière de sécurité des réseaux et des systèmes d'information, prévoyant notamment les rôles et les responsabilités des organismes publics et des autres acteurs pertinents ;

c) l'inventaire des mesures en matière de préparation, d'intervention et de récupération, y compris la coopération entre les secteurs public et privé ;

d) un aperçu des programmes d'éducation, de sensibilisation et de formation en rapport avec la stratégie nationale en matière de sécurité des réseaux et des systèmes d'information ;

e) un aperçu des plans de recherche et de développement en rapport avec la stratégie nationale en matière de sécurité des réseaux et des systèmes d'information ;

f) un plan d'évaluation des risques permettant d'identifier les risques ;

g) une liste des différents acteurs concernés par la mise en œuvre de la stratégie nationale en matière de sécurité des réseaux et des systèmes d'information. »

Art. 16. La présente loi entre en vigueur le premier jour du deuxième mois qui suit sa publication au Journal officiel du Grand-Duché de Luxembourg.

Mandons et ordonnons que la présente loi soit insérée au Journal officiel du Grand-Duché de Luxembourg pour être exécutée et observée par tous ceux que la chose concerne.

*

ANNEXE

Types d'entités aux fins de l'article 1, point 3.

Secteur	*Sous-secteur*	*Type d'entités*
1. Energie	a) Electricité	– Entreprises d'électricité au sens de l'article 1er, paragraphe 14, de la loi modifiée du 1er août 2007 relative à l'organisation du marché de l'électricité, qui remplit la fonction de « fourniture » au sens de l'article 1er, paragraphe 21, de la même loi
		– Gestionnaires de réseau de distribution au sens de l'article 1er, paragraphe 24, de la loi modifiée du 1er août 2007 relative à l'organisation du marché de l'électricité
		– Gestionnaires de réseau de transport au sens de l'article 1er, paragraphe 25, de la loi modifiée du 1er août 2007 relative à l'organisation du marché de l'électricité
	b) Pétrole	– Exploitants d'oléoducs
		– Exploitants d'installations de production, de raffinage, de traitement, de stockage et de transport de pétrole
	c) Gaz	– Entreprises de fourniture au sens de l'article 1er, paragraphe 14, de la loi modifiée du 1er août 2007 relative à l'organisation du marché du gaz naturel
		– Gestionnaires de réseau de distribution au sens de l'article 1er, paragraphe 22, de la loi modifiée du 1er août 2007 relative à l'organisation du marché du gaz naturel
		– Gestionnaires de réseau de transport au sens de l'article 1er, paragraphe 24, de la loi modifiée du 1er août 2007 relative à l'organisation du marché du gaz naturel
		– Gestionnaires d'installation de stockage au sens de l'article 1er, paragraphe 25, de la loi modifiée du 1er août 2007 relative à l'organisation du marché du gaz naturel
		– Gestionnaires d'installation de GNL au sens de l'article 1er, paragraphe 23, de la loi modifiée du 1er août 2007 relative à l'organisation du marché du gaz naturel
		– Entreprises de gaz naturel au sens de l'article 1er, paragraphe 15, de la loi modifiée du 1er août 2007 relative à l'organisation du marché du gaz naturel
		– Exploitants d'installations de raffinage et de traitement de gaz naturel

Secteur	*Sous-secteur*	*Type d'entités*
2. Transports	a) Transport aérien	– Transporteurs aériens au sens de l'article 3, point 4), du règlement (CE) n° 300/2008 du Parlement européen et du Conseil du 11 mars 2008 relatif à l'instauration de règles communes dans le domaine de la sûreté de l'aviation civile et abrogeant le règlement (CE) no 2320/2002
		– Entités gestionnaires d'aéroports au sens de l'article 2, point 1), de la loi du 23 mai 2012 portant transposition de la directive 2009/12/CE du Parlement européen et du Conseil du 11 mars 2009 sur les redevances aéroportuaires et portant modification: 1) de la loi modifiée du 31 janvier 1948 relative à la réglementation de la navigation aérienne; 2) de la loi modifiée du 19 mai 1999 ayant pour objet a) de réglementer l'accès au marché de l'assistance en escale à l'aéroport de Luxembourg, b) de créer un cadre réglementaire dans le domaine de la sûreté de l'aviation civile, et c) d'instituer une Direction de l'Aviation Civile, aéroports, y compris les aéroports du réseau central énumérés à l'annexe II, section 2, du règlement (UE) n° 1315/2013 du Parlement européen et du Conseil du 11 décembre 2013 sur les orientations de l'Union pour le développement du réseau transeuropéen de transport et abrogeant la décision no 661/2010/UE, et entités exploitant les installations annexes se trouvant dans les aéroports
		– Services du contrôle de la circulation aérienne au sens de l'article 2, point 1., du règlement (CE) n° 549/2004 du Parlement européen et du Conseil du 10 mars 2004 fixant le cadre pour la réalisation du ciel unique européen (« règlement–cadre »)
	b) Transport ferroviaire	– Gestionnaires de l'infrastructure au sens de l'article 2, point 3., de la loi modifiée du 10 mai 1995 relative à la gestion de l'infrastructure ferroviaire
		– Entreprises ferroviaires au sens de l'article 2, point 7., de la loi modifiée du 11 juin 1999 relative à l'accès à l'infrastructure ferroviaire et à son utilisation, y compris les exploitants d'installations de services au sens de l'article 2, point 2., de la loi modifiée du 10 mai 1995 relative à la gestion de l'infrastructure ferroviaire
	c) Transport par voie d'eau	– Sociétés de transport terrestre, maritime et côtier de passagers et de fret au sens de l'annexe I du règlement (CE) n° 725/2004 du Parlement européen et du Conseil du 21 novembre 2012 établissant un espace ferroviaire unique européen, à l'exclusion des navires exploités à titre individuel par ces sociétés
		– Entités gestionnaires des ports au sens de l'article 3, point 1., de la directive 2005/65/CE du Parlement européen et du Conseil du 26 octobre 2005 relative à l'amélioration de la sûreté des ports, y compris les installations portuaires au sens de l'article 2, point 11., du règlement (CE) n° 725/2004, ainsi que les entités exploitant des ateliers et des équipements à l'intérieur des ports
		– Exploitants de services de trafic maritime au sens de l'article 2, lettre o), du règlement grand–ducal modifié du 27 février 2011 relatif à la mise en place d'un système communautaire de suivi du trafic des navires et d'information

Secteur	*Sous-secteur*	*Type d'entités*
	d) Transport routier	– Autorités routières au sens de l'article 2, point 12., du règlement délégué (UE) 2015/962 de la Commission du 18 décembre 2014 complétant la directive 2010/40/UE du Parlement européen et du Conseil en ce qui concerne la mise à disposition, dans l'ensemble de l'Union, de services d'informations en temps réel sur la circulation, chargées du contrôle de gestion du trafic
		– Exploitants de systèmes de transport intelligents au sens de la lettre circulaire du 22 février 2012 concernant la directive 2010/40/UE du Parlement européen et du Conseil du 7 juillet 2010 concernant le cadre pour le déploiement de systèmes de transport intelligents dans le domaine du transport routier et d'interfaces avec d'autres modes de transport
3. Banques		– Etablissements de crédit au sens de l'article 1er, point 12), de la loi modifiée du 5 avril 1993 relative au secteur financier
4. Infrastructures de marchés financiers		– Exploitants de plate–forme de négociation au sens de l'article 4, point 24., de la directive 2014/65/UE du Parlement européen et du Conseil du 15 mai 2014 concernant les marchés d'instruments financiers et modifiant la directive 2002/92/CE et la directive 2011/61/UE
		– Contreparties centrales au sens de l'article 2, point 1., du règlement (UE) n° 648/2012 du Parlement européen et du Conseil du 4 juillet 2012 sur les produits dérivés de gré à gré, les contreparties centrales et les référentiels centraux
5. Secteur de la santé	Etablissements de soins de santé (y compris les hôpitaux et les cliniques privées)	– Prestataires de soins de santé au sens de l'article 2, lettre f), de la loi du 24 juillet 2014 relative aux droits et obligations du patient, portant création d'un service national d'information et de médiation dans le domaine de la santé et modifiant: – la loi modifiée du 28 août 1998 sur les établissements hospitaliers; – la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel; – le Code civil
6. Fourniture et distribution d'eau potable		– Fournisseurs et distributeurs d'eaux destinées à la consommation humaine au sens de l'article 3, point 1), lettre a), du règlement grand–ducal modifié du 7 octobre 2002 relatif à la qualité des eaux destinées à la consommation humaine
7. Infrastructures numériques		– IXP
		– Fournisseurs de services DNS
		– Registres de noms de domaines de haut niveau

*

EXPOSE DES MOTIFS

Le projet de loi se propose de 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 (*Directive on security of network and information systems*, ci-après directive « NIS »).[1]

Cette directive est considérée comme une pierre angulaire de la réponse apportée par l'Union européenne aux menaces et défis cybernétiques croissants qui accompagnent la numérisation de notre vie économique.[2] En effet, elle s'inscrit dans l'ère de la numérisation générale où un rôle crucial est accordé aux réseaux et systèmes d'information qui ont évolué en éléments-clé du fonctionnement économique et social de nos sociétés. Au vu des incidents de sécurité dont l'ampleur, la fréquence et l'impact ne cesse de croître, il est devenu apparent que ces réseaux et systèmes d'information nécessitent une protection spéciale et harmonisée à travers les Etats membres de l'Union qui sont loin de présenter le même niveau de préparation face aux cybermenaces.

Ainsi, la directive a pour objet de renforcer l'harmonisation et la coopération en matière de gestion des risques cyber. Elle dépasse la démarche poursuivie jusqu'à présente et consistant à fixer des règles de sécurité minimales à respecter dans différents secteurs tels que le secteur des banques, le secteur des marchés financiers ou encore le secteur des communications électroniques. Elle prévoit ainsi des règles horizontales de gestion des risques minimales à respecter par chaque Etat membre par rapport à la sécurité des réseaux et des systèmes d'information des opérateurs fournissant des services essentiels et des fournisseurs de service numérique. La directive cite les secteurs considérés comme particulièrement nécessaires au fonctionnement de la société, à savoir les secteurs de l'énergie, des transports, des banques, des infrastructures de marchés financiers, de la santé, de la fourniture et distribution d'eau potable et des infrastructures numériques.

En mettant en place des exigences minimales communes visant d'assurer un niveau élevé en matière de sécurité des réseaux, la directive aborde le sujet de la cybersécurité sous différents angles, à savoir :

– le renforcement de la sécurité des systèmes d'information des « opérateurs de services essentiels » à travers la définition au niveau national de règles de cybersécurité auxquelles les opérateurs devront se conformer et l'obligation pour ces derniers de notifier les incidents ayant un impact sur la continuité de leurs services essentiels ;
– l'instauration de règles européennes communes en matière de cybersécurité des « fournisseurs de service numérique » dans les domaines de l'informatique en nuage, des moteurs de recherche et places de marché en ligne ;
– le renforcement des capacités nationales de gestion et de promotion du sujet de la cybersécurité en demandant aux Etats membres de se doter d'une autorité nationale compétente pour assurer la sécurité des réseaux et systèmes d'information des opérateurs considérés comme essentiels, d'équipes nationales de réponse aux incidents informatiques et d'une stratégie nationale de cybersécurité ;
– l'établissement d'un cadre de coopération entre Etats membres de l'Union européenne par le biais de la création d'un « groupe de coopération » des Etats membres pour s'échanger sur le sujet de la cybersécurité d'une part et par la mise en place d'un « réseau européen des CSIRT » pour faciliter le partage d'informations techniques sur les risques et vulnérabilités.

1. La promotion d'une culture de gestion des risques

D'abord, la directive promeut une culture de gestion des risques impliquant une analyse des risques et l'application de mesures de sécurité adaptées aux risques encourus en édictant des exigences en matière de sécurité et de notification des incidents pour les acteurs économiques les plus importants, à savoir les opérateurs de services essentiels (OSE) et les fournisseurs de service numérique (FSN, *digital service providers*).

---

1 *J.O.U.E.*, L 194 du 19 juillet 2016, p. 1.

2 Communication de la Commission au Parlement européen et au Conseil, « Exploiter tout le potentiel de la directive SRI – Vers la mise en œuvre effective de 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, *C.O.M.* (2017) 476 final, p. 2.

– Par « **opérateur de services essentiels** », les institutions européennes entendent toute entreprise qui joue un rôle important pour la société et l'économie, et qui agit dans un des secteurs suivants : l'énergie (électricité, pétrole et gaz), les transports (aérien, ferroviaire, par voie d'eau et routier), les services bancaires (établissements de crédit), les infrastructures de marchés financiers (plateformes de négociation, contreparties centrales), la santé (prestataires de soins de santé), l'eau (fourniture et distribution d'eau potable) ou encore les infrastructures numériques.

  La désignation d'un OSE se fait sur base d'un triple critère :

  ° Il s'agit d'une entité qui fournit, dans un des secteurs susmentionnés, un service qui est essentiel au maintien de fonctions sociétales et économiques critiques.

  ° La fourniture de ce service doit être tributaire des réseaux et des systèmes d'information.

  ° Un incident doit avoir un effet disruptif important sur la fourniture dudit service.

  Par analogie à la démarche choisie par la Commission européennes dans d'autres secteurs, comme par exemple dans le contexte de la directive modifiée 2002/21/CE relative à un cadre réglementaire commun pour les réseaux et services de communications électroniques[3] ou encore la directive 2014/65/UE concernant les marchés d'instruments financiers[4], les OSE sont tenus de prendre les mesures techniques organisationnelles nécessaires pour gérer les risques qui menacent la sécurité des réseaux et des systèmes d'information pour la fourniture de leurs services. Ces mesures doivent contribuer à prévenir un incident et à en limiter l'impact. En plus, les OSE sont soumis à une obligation de notification en ce qui concerne les incidents qui ont un impact significatif sur la continuité des services essentiels qu'ils fournissent.

  Notons dans ce contexte que la notion d'OSE ne doit pas être confondue avec la notion d'« opérateur d'une infrastructure critique » (OIC), telle que prévue par la loi portant création d'un Haut-Commissariat à la Protection nationale[5], même si des recoupements partiels ne peuvent être exclus et qu'une entité pourrait être considérée à la fois comme OSE et comme OSI.

  Ainsi, le concept de protection d'une infrastructure critique englobe une infrastructure dans son entièreté avec à gérer, au-delà du dysfonctionnement des réseaux et systèmes d'information, tous les risques pouvant affecter la continuité des activités d'une infrastructure critique comme les risques d'origine naturelle, environnementale et sanitaire (p.ex. intempéries graves, inondations, pandémies,…), les risques d'origine technologique (p.ex. défaillance d'un processus, rupture de l'alimentation en énergie, dysfonctionnement des systèmes informatiques, etc…) ou encore les risques d'actes malveillants (p.ex. attaque cyber, intrusion, sabotage, attaques terroriste, etc…).

  La notion d'infrastructure critique est dès lors une notion beaucoup plus vaste que celle d'OSE qui se focalise d'une part sur le risque lié au dysfonctionnement des systèmes informatiques et d'autre part sur une partie des services fournis par l'entité en question, en l'occurrence les services essentiels (par opposition à des services non essentiels). De la sorte, alors qu'un aéroport est à considérer comme une infrastructure critique au sens des dispositions afférentes de la loi portant organisation du Haut-Commissariat à la Protection nationale, seuls certains services fournis par l'aéroport sont à considérer comme services essentiels au sens de la directive NIS. Par exemple, la gestion des pistes pourrait être considérée comme service essentiel, alors que la mise à disposition de zones commerciales serait un service non essentiel.[6]

  En outre, la directive NIS accorde à l'autorité qui est chargée de veiller au respect des mesures de sécurité des OSE et des FSN des compétences qui vont largement au-delà des compétences que la loi concède au Haut-Commissariat à la Protection nationale en matière des OIC. Ainsi, la directive NIS permet à l'autorité compétente, à l'instar des pouvoirs conférés aux autorités de régulation dans d'autres secteurs comme dans celui de la surveillance des communications électroniques (ILR) ou de la surveillance des banques (CSSF), de formuler des instructions contraignantes à l'égard des OSE, alors que le Haut-Commissariat à la Protection nationale ne peut que faire des recommanda-

---

3 Loi modifiée du 27 février 2011 sur les réseaux et services de communications électroniques, *Mém. A* n° 43, 8 mars 2011, p. 610.

4 Projet de loi n°7157.

5 Art. 2, 4. de la loi du 23 juillet 2016 portant création d'un Haut-Commissariat à la Protection nationale : « tout point, système ou partie de celui-ci qui est indispensable à la sauvegarde des intérêts vitaux ou des besoins essentiels de tout ou partie du pays ou de la population ou qui est susceptible de faire l'objet d'une menace particulière »

6 Consid. (22) Directive NIS.

tions à l'égard des OIC. De plus, la directive NIS confère à l'autorité compétente un véritable pouvoir de sanction à l'égard des OSE, tandis que le Haut-Commissariat à la Protection nationale ne dispose pas de ce pouvoir de sanction dans le cadre de sa mission de protection des infrastructures critiques.

Afin d'éviter cependant que des opérateurs qui sont à la fois des OIC et des OSE ne soient pénalisés par leur double statut, l'ILR, la CSSF, la CNPD et le Haut-Commissariat à la Protection nationale visent à mettre en place une plateforme de notification unique afin d'alléger la charge administrative des entités devant notifier un incident. Une telle plateforme de notification unique, permettrait à l'opérateur, confronté à un incident d'une certaine envergure, de ne faire qu'une seule notification, celle-ci étant par la suite transmise de manière automatique aux autorités concernées par l'incident.

– À côté des exigences de sécurité et de notification imposées aux OSE, la directive NIS instaure des règles communes en matière de cybersécurité à respecter par les **fournisseurs de service numérique**, c'est-à-dire les places de marché en ligne, les moteurs de recherche en ligne, ainsi que les services d'informatique en nuage.

  • La place de marché en ligne fournit aux entreprises l'infrastructure de base pour le commerce en ligne et transfrontalier. Elle permet aux consommateurs et aux professionnels de conclure des contrats de vente ou de service en ligne avec des professionnels et c'est la destination finale pour la conclusion desdits contrats. Ainsi, *E-bay* ou les magasins d'applications en ligne seraient à considérer comme places de marché en ligne, tandis que des intermédiaires de services tiers tels que *Skyscanner* et les services de comparaison de prix, qui redirigent l'utilisateur vers le site internet du professionnel où le contrat de service ou de produit est effectivement conclu, ne tombent pas sous l'égide de la directive NIS.[7]

  • Un moteur de recherche en ligne est 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 base d'une requête lancée sur n'importe quel sujet.[8] Tandis que le moteur de recherche de *EURLEX* ne serait pas visé par la présente directive puisqu'il effectue ses recherches sur un site internet déterminé, *Google* devrait être considéré comme fournisseur de service numérique.

  • L'informatique en nuage peut être décrite comme un type particulier de service informatique qui utilise des ressources partagées pour traiter des données à la demande, les ressources partagées désignant tout type de composants matériels ou logiciels (réseaux, serveurs ou autres infrastructures, stockage, applications, et services) mis à la disposition des utilisateurs à la demande pour le traitement des données.

  Vu que certains services numériques pourraient représenter une ressource importance pour leurs utilisateurs, il faut que ces entités mettent en place un système efficace de gestion des risques et de notification des incidents, tout en sachant que la directive estime que le degré de risque est plus élevé pour les OSE que pour les FSN et que par conséquent, les exigences en matière de sécurité imposées aux FSN devraient être moins strictes.[9]

Enfin, remarquons que les dispositions relatives aux exigences de sécurité et/ou de notification applicables aux FSN ou aux OSE en vertu de la directive ne sont pas applicables si une législation sectorielle de l'Union prévoit des exigences de sécurité et/ou de notification qui ont un effet au moins équivalent à celui des obligations correspondantes de la directive NIS.[10] Par exemple, en ce qui concerne les infrastructures de marchés financiers, la directive NIS ne s'appliquera pas aux contreparties centrales[11] et dans le secteur bancaire, la prestation de services de paiement par les établissements

---

7 Annexe de la communication de la Commission au Parlement européen et au Conseil, « Exploiter tout le potentiel de la directive SRI – Vers la mise en œuvre effective de 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, *C.O.M.* (2017) 476 final, p. 33.

8 *Ibid*., p. 34.

9 *J.O.U.E.*, L 194 du 19 juillet 2016, p. 1, consid. (49).

10 Art. 1er, (7) Directive NIS.

11 Réglementées par le règlement (UE) n° 648/2012 du Parlement européen et du Conseil du 4 juillet 2012 sur les produits dérivés de gré à gré, les contreparties centrales et les référentiels centraux, *J.O.U.E.*, L 201 du 27 juillet 2012, p. 1.

de crédit[12] ne tombera pas sous le champ d'application de la directive NIS. En outre, la directive NIS exclut expressément les fournisseurs de services de télécommunications et les prestataires de services de confiance.[13]

2. La préparation des Etats membres aux défis cybernétiques

Ensuite, la directive comporte des dispositions qui imposent certaines obligations aux Etats membres en vue d'augmenter la résilience face aux menaces et défis cybernétiques croissants. Ainsi, les Etats membres désignent une ou plusieurs autorités nationales compétentes, mettent en place un point de contact national unique compétent en matière de coopération transfrontalière et adoptent une stratégie nationale en matière de sécurité des réseaux et des systèmes d'information.

– Sur un plan national, l'Institut luxembourgeois de régulation (ILR), ensemble avec la Commission de surveillance du secteur financier (CSSF), seront à considérer comme **autorités nationales compétentes** chargées d'accomplir les tâches liées à la sécurité des réseaux et des systèmes d'information des OSE et des FSN. Puisque la directive pose que la compétence des autorités compétentes s'étend sur au moins sept secteurs (énergie, transports, banques, infrastructures de marchés financiers, santé, fourniture et distribution d'eau potable et infrastructures numériques) et que l'ILR régule d'ores et déjà une grande partie de ces secteurs, tout en disposant d'une expertise confirmée en matière de régulation, ainsi que d'un statut d'indépendance, il appert cohérent de lui confier la mission d'autorité compétente dans le sens de la directive NIS, à l'exception des secteurs des banques et des infrastructures de marchés financiers, où la CSSF restera l'autorité régulatrice. Confier la mission d'autorité compétente à une nouvelle entité, étrangère aux secteurs définis dans la directive NIS, aurait nécessairement résulté en une interférence avec les attributions des autorités de régulation existantes.

  En outre, il faut souligner que la compétence de l'ILR d'assurer cette nouvelle mission se confirme d'autant plus par sa compétence actuelle dans le domaine des communications électroniques. Effectivement, l'approche de la directive NIS qui oblige les Etats membres à assurer que les OSE prennent les mesures nécessaires pour assurer un niveau de protection élevé des systèmes d'information et pour réduire ainsi les conséquences d'un éventuel incident de sécurité, n'est nullement nouvelle. Un libellé quasiment identique peut être retrouvé dans la directive 2009/140/CE sur les communications électroniques,[14] transposé en droit luxembourgeois par la loi modifiée du 27 février 2011 sur les réseaux et services de communications électroniques qui attribue une compétences générale en la matière à l'ILR.

  Enfin, la directive NIS permet aux autorités compétentes de formuler des instructions contraignantes à l'égard des OSE tout en leur conférant un véritable pouvoir de sanction. De par leurs missions et leur statut légal actuel de régulateurs, l'ILR et la CSSF ont su acquérir le savoir-faire nécessaire leur permettant d'assumer cette nouvelle mission.

– Dans la même lignée, l'ILR est à considérer comme **point de contact national unique** dans le cadre de la directive NIS. Ainsi, il reviendra à l'ILR de coordonner les tâches liées à la sécurité des réseaux et des systèmes d'information et d'assurer la coopération transfrontalière en la matière.

– Le troisième volet de la préparation étatique face aux cybermenaces veut que les Etats se dotent d'une **stratégie nationale en matière de sécurité des réseaux et des systèmes d'information** définissant les objectifs stratégiques et les actions politiques concrètes à mettre en œuvre. Vu que cette stratégie nationale en matière de sécurité des réseaux et des systèmes d'information peut être considérée comme équivalente à une stratégie nationale de cybersécurité[15] et que le Luxembourg dispose déjà d'une telle stratégie nationale en matière de cybersécurité élaborée par un comité

---

12 Réglementée par la directive (UE) 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015 concernant les services de paiement dans le marché intérieur, modifiant les directives 2002/65/CE, 2009/110/CE et 2013/36/UE et le règlement (UE) n° 1093/2010, et abrogeant la directive 2007/64/CE, *J.O.U.E.*, L 337 du 23 décembre 2015, p. 35.

13 Art. 1er, (3) Directive NIS.

14 Art. 13*bis* de la directive 2009/140/CE du Parlement européen et du Conseil du 25 novembre 2009 modifiant les directives 2002/21/CE relative à un cadre réglementaire commun pour les réseaux et services de communications électroniques, 2002/19/CE relative à l'accès aux réseaux de communications électroniques et aux ressources associées, ainsi qu'à leur interconnexion, et 2002/20/CE relative à l'autorisation des réseaux et services de communications électroniques, *J.O.U.E.*, L 337 du 18 décembre 2009, p. 37.

15 Annexe de la communication de la Commission au Parlement européen et au Conseil, *o.c.*, (v. note 7), p. 5.

interministériel présidé par le Haut-Commissariat à la Protection nationale (HCPN), la nouvelle loi fortifie ce rôle de coordinateur en lui accordant une assise juridique dans la loi HCPN. Notons que la troisième version de la stratégie nationale en matière de cybersécurité verra le jour en 2018.

3. Le renforcement de la coopération entre Etats membres

Enfin, le troisième grand objectif de la directive est de renforcer la coopération et l'échange d'informations sur un niveau européen en instituant un groupe de coopération et un réseau des centres de réponse aux incidents de sécurité informatiques (« réseau des CSIRT »).

– Le **groupe de coopération** sert comme forum européen d'échange de savoir-faire et de bonnes pratiques en réunissant des représentants des Etats membres, de la Commission et de l'Agence de l'Union européenne chargée de la sécurité des réseaux et de l'information (ENISA). Il a pour mission de soutenir et de favoriser la coopération stratégique entre les Etats membres, de faciliter l'échange d'informations et de renforcer la confiance mutuelle.

  À titre d'exemple, ce groupe aide les Etats membres à suivre une approche cohérente dans le processus d'identification des opérateurs de services essentiels. Il est chargé de fournir des orientations stratégiques, d'évaluer les stratégies nationales mises en place par les Etats membres en matière de sécurité, ou encore plus généralement d'échanger sur les bonnes pratiques dans le domaine de la sécurité informatique.

– Le **réseau des CSIRT** promeut une coopération opérationnelle rapide et effective entre Etats membres. Dans ce sens, chaque Etat membre doit désigner un ou plusieurs CSIRT qui représentent le Luxembourg au sein du réseau des CSIRT. Au Luxembourg, la fonction de CSIRT est assurée communément par le *Computer Emergency Response Team Gouvernemental* (GovCERT) et le *Computer Incident Response Centre Luxembourg* (CIRCL) chargés de la gestion des incidents.

  Le réseau des CSIRT doit contribuer au renforcement de la confiance entre les Etats membres et « promouvoir une coopération rapide et effective au niveau opérationnel »[16] en aidant les Etats membres à faire face aux incidents transfrontaliers. Le secrétariat du réseau des CSIRT tient à jour un site internet mettant à la disposition du public des informations générales sur les principaux incidents qui sont survenus dans toute l'Union.

Puisque les dispositions de la directive concernant le groupe de coopération et le réseau des CSIRT suffisent à elles-mêmes, elles n'ont pas été transposées en droit luxembourgeois.

*

COMMENTAIRE DES ARTICLES

Ad article 1er

L'article 1er reprend la définition des termes employés dans la présente loi. Remarquons que la quasi-totalité des définitions font preuve d'une transposition fidèle de la directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union (*Directive on security of network and information systems*, ci-après directive « NIS »).[17]

La définition sous l'article 1er, point 1., énonce ce que la loi comprend par « réseau et système d'information ». Le législateur européen a choisi de définir ces termes de manière large et ainsi, pourraient notamment tomber sous le champ d'application de la loi, les *Industrial Control Systems* (ICS), tel que SCADA (système d'acquisition et de contrôle de données).

Le troisième point de l'article 1er définit l'opérateur de services essentiels, qui constitue, ensemble avec les fournisseurs de service numérique, l'un des acteurs principaux de la directive NIS. Un opérateur de services essentiels (OSE) est une entité qui joue un rôle important pour la société et l'économie et qui agit dans un des secteurs mentionnés en annexe (énergie (électricité, pétrole et gaz), transports (aérien, ferroviaire, par voie d'eau et routier), services bancaires (établissements de crédit), infrastruc-

16 Art. 1er, (2), c) Directive NIS.

17 *J.O.U.E.*, L 194 du 19 juillet 2016, p. 1.

tures de marchés financiers (plateformes de négociation, contreparties centrales), santé (prestataires de soins de santé), eau (fourniture et distribution d'eau potable), infrastructures numériques)).

Tous les OSE qui ont leur établissement sur le territoire luxembourgeois tombent sous l'égide de la présente loi. L'article sous rubrique fait abstraction de la forme juridique de cet établissement afin d'être conforme à la directive 2016/1148 qui rattache la compétence territoriale d'un Etat membre à l'exercice effectif et réel d'une activité au moyen d'une installation stable, peu importe sa forme juridique.[18]

En ce sens, les autorités luxembourgeoises peuvent être compétentes à l'égard d'un OSE non seulement dans les cas où l'opérateur a son siège social sur le territoire luxembourgeois, mais aussi dans les cas où l'opérateur a, par exemple, une succursale, une filiale ou un autre type d'établissement juridique sur le territoire du Grand-Duché. Il en résulte que plusieurs Etats membres en parallèle pourraient avoir compétence sur la même entité.[19]

Les fournisseurs de services numériques définis au point 5., constituent le deuxième destinataire de la directive NIS. Ces entités sont considérées comme des acteurs économiques importants du fait qu'elles sont utilisées par de nombreuses entreprises pour la fourniture de leurs propres services, et qu'une perturbation du service numérique pourrait avoir une incidence sur des fonctions économiques et sociétales clés.[20]

Afin de tomber sous l'égide de la loi, ces personnes morales doivent fournir un service numérique du type « place de marché en ligne », « moteur de recherche en ligne » ou « service informatique en nuage ».[21]

La douzième définition sous l'article 1er explique le terme « point d'échange Internet », structure de réseau qui permet l'interconnexion d'au moins deux systèmes techniquement autonomes, essentiellement aux fins de faciliter l'échange de trafic internet. Le point d'échange internet constitue le lieu physique où un certain nombre de réseaux peuvent échanger du trafic internet entre eux par l'intermédiaire d'un commutateur. Le fournisseur IXP n'est normalement pas responsable de l'acheminement du trafic internet qui est effectué par les fournisseurs de réseau.[22]

Notons qu'un IXP ne fournit pas d'accès à un réseau et n'agit pas en tant que fournisseur ou opérateur de transit. Cette dernière catégorie de fournisseurs est constituée par les entreprises fournissant des réseaux et/ou des services de communications publics qui sont soumises aux obligations de sécurité et de notification prévues aux articles 45 et 46 de la loi modifiée du 27 février 2011 sur les réseaux et les services de communications électroniques.[23]

Le « système de noms de domaine » (DNS), défini à l'article 1er, point 13., peut être décrit comme un système hiérarchique et distribué d'affectation de noms pour les ordinateurs, les services ou toute autre ressource connectée à internet et qui permet l'encodage des noms de domaine en adresses IP (*Internet Protocol*). Le rôle principal du système est donc de traduire les noms de domaine assignés en adresses IP. Afin de permettre ce type de « traduction » des noms de domaine en adresses IP opérationnelles, le DNS exploite une base de données et utilise des serveurs de noms et un résolveur.[24]

Selon l'article 1er, point 15., le « registre de noms de domaine de haut niveau » (TLD) est une entité qui administre et gère l'enregistrement de noms de domaine internet dans un domaine de haut niveau. L'administration et la gestion des noms de domaine comprennent l'encodage des noms de domaines de haut niveau en adresses IP.[25]

Une tâche importante des registres consiste à attribuer des noms de deuxième niveau aux titulaires sous leurs domaines de haut niveau respectifs. Ces titulaires peuvent également, s'ils le souhaitent,

---

18 Consid. (21) Directive NIS.

19 Annexe de la communication de la Commission au Parlement européen et au Conseil, « Exploiter tout le potentiel de la directive SRI – Vers la mise en œuvre effective de 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 », *C.O.M.* (2017) 476 final, p. 25.

20 *Ibid.*, p. 32.

21 Voir article 1er, 16., 17., 18. pour la définition de ces termes.

22 Annexe de la communication de la Commission au Parlement européen et au Conseil, *o.c.*, (v. note 19), p. 21.

23 *Ibid.*, p. 22.

24 *Ibid.*, p. 22.

25 *Ibid.*, p. 22.

attribuer eux-mêmes des noms de domaine de troisième niveau. Les noms de domaines nationaux de haut niveau sont désignés pour représenter un pays ou un territoire selon la norme ISO 3166-1 (par exemple « .lu »). Les noms de domaines de haut niveau « génériques » (par exemple « .com ») n'ont normalement pas de désignation géographique ou de pays.[26]

Il convient de noter que l'exploitation d'un registre de noms de domaine de haut niveau peut supposer la fourniture de DNS. Ainsi, conformément aux règles de délégation de l'IANA (*Internet Assigned Numbers Authority*), l'entité désignée traitant des noms de domaines nationaux de haut niveau doit – entre autres – superviser les noms de domaine et exploiter le DNS de ce pays.[27]

La place de marché en ligne, définie par le point 16. de l'article 1er, constitue un des trois services numériques énumérés par la directive. La place de marché en ligne fournit aux entreprises l'infrastructure de base pour le commerce en ligne et transfrontalier en permettant notamment aux PME d'accéder au marché unique numérique de l'Union au sens large. Elle permet aux consommateurs et aux professionnels de conclure des contrats de vente ou de service en ligne avec des professionnels.[28]

Ne sont pas visés les services en ligne qui ne servent que d'intermédiaires pour des services fournis par un tiers à travers lequel un contrat peut être conclu. Elle ne concerne donc pas les services en ligne qui comparent le prix de certains produits ou services de plusieurs professionnels, avant de réorienter l'utilisateur vers le professionnel choisi en vue de l'achat du produit.[29] Ainsi, *E-bay* ou les magasins d'applications en ligne seraient à considérer comme places de marché en ligne, tandis que des intermédiaires de services tiers tels que *Skyscanner* et les services de comparaison de prix, qui redirigent l'utilisateur vers le site internet du professionnel où le contrat de service ou de produit est effectivement conclu, ne tombent pas sous l'égide de la directive NIS.[30]

Notons que parmi les services informatiques fournis par la place de marché en ligne peuvent figurer la facilitation de recherche de produits appropriés, la fourniture de produits, l'expertise transactionnelle et la mise en relation des acheteurs et des vendeurs.[31]

Le moteur de recherche en ligne constitue le deuxième type de service numérique visé par la directive NIS (article 1er, point, 17.). Un moteur de recherche en ligne est 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 base d'une requête lancée sur n'importe quel sujet.[32] Tandis que le moteur de recherche de *EURLEX* ne serait pas ciblé par la présente directive puisqu'il effectue ses recherches sur un site internet déterminé, *Google* devrait être considéré comme fournisseur de service numérique. Ne sont pas non plus couverts par la définition, les services en ligne qui comparent les prix de certains produits ou services de différents professionnels et qui réorientent ensuite l'utilisateur vers le professionnel choisi en vue de l'achat du produit.[33]

Le point 18. de l'article 1er décrit le troisième type de service numérique tombant sous le champ d'application de la présente loi. Le service informatique en nuage peut être décrit comme un service informatique qui utilise des ressources partagées pour traiter des données à la demande. Les ressources partagées désignent tout type de composants matériels ou logiciels (réseaux, serveurs ou autres infrastructures, stockage, applications, et services) mis à la disposition des utilisateurs à la demande pour le traitement des données.[34]

– Le terme « modulable » renvoie aux ressources informatiques qui sont attribuées d'une manière souple par le fournisseur de services en nuage, indépendamment de la localisation géographique de ces ressources, pour gérer les fluctuations de la demande.[35]
– Les termes « ensemble variable » sont utilisés pour décrire les ressources informatiques qui sont mobilisées et libérées en fonction de la demande pour pouvoir augmenter ou réduire rapidement les

---

26 *Ibid.*, p. 23.

27 Annexe de la communication de la Commission au Parlement européen et au Conseil, *o.c.*, (v. note 19), p. 23.

28 *Ibid.*, p. 33.

29 Consid. (15) Directive NIS.

30 Annexe de la communication de la Commission au Parlement européen et au Conseil, *o.c.*, (v. note 19), p. 33.

31 *Ibid.*, p. 33.

32 *Ibid.*, p. 34.

33 Consid. (16) Directive NIS.

34 Annexe de la communication de la Commission au Parlement européen et au Conseil, *o.c.*, (v. note 19), p. 34.

35 Consid. (17) Directive NIS.

ressources disponibles en fonction de la charge de travail,[36] de telle sorte qu'à chaque instant les ressources disponibles correspondent le plus possible à la demande actuelle.

– Les termes « pouvant être partagées » sont utilisés pour décrire les ressources informatiques qui sont mises à disposition de nombreux utilisateurs qui partagent un accès commun au service. Bien que le service soit fourni à partir du même équipement électronique, le traitement est effectué séparément pour chaque utilisateur.[37]

Afin de faciliter la compréhension de la loi, la définition de l'autorité compétente concernée a été insérée au début du texte (article 1er, point 19.) et constitue dès lors, au niveau des définitions, un ajout par rapport au texte de la directive NIS.

Au Luxembourg, l'Institut luxembourgeois de régulation (ILR), ensemble avec la Commission de surveillance du secteur financier (CSSF), sont les autorités nationales compétentes chargées d'accomplir les tâches liées à la sécurité des réseaux et des systèmes d'information des OSE et des FSN. Puisque la directive pose que la compétence des autorités compétentes sur les OSE s'étend sur au moins sept secteurs (énergie, transports, banques, infrastructures de marchés financiers, santé, fourniture et distribution d'eau potable et infrastructures numériques) et que l'ILR régule d'ores et déjà une grande partie de ces secteurs, tout en disposant d'une expertise confirmée en matière de régulation, ainsi que d'un statut d'indépendance, il appert cohérent de lui confier la mission d'autorité compétente dans le sens de la directive NIS, à l'exception des secteurs des banques et des infrastructures de marchés financiers, où la CSSF restera l'autorité régulatrice. Confier la mission d'autorité compétente à une nouvelle entité, étrangère aux secteurs définis dans la directive NIS, aurait nécessairement résulté en une interférence avec les attributions des autorités de régulation existantes.

De même, en matière de FSN, la CSSF sera compétente en matière de services numériques fournis par des entités tombant sous sa surveillance, tandis que l'ILR couvre tous les autres FSN, indépendamment de leur secteur d'activité. Ceci permettra notamment à la CSSF de rester compétente pour les PSF de support qui offrent des services en nuage.

Conformément à l'article 1er, point 20., le point de contact national unique a pour mission de coordonner les tâches liées à la sécurité des réseaux et des systèmes d'information et de gérer la coopération transfrontalière avec les autorités compétentes des autres Etats membres, le groupe de coopération et le réseau des CSIRT. En outre, la directive NIS prévoit que le point de contact unique transmet annuellement au groupe de coopération un rapport de synthèse sur les notifications reçues par les autorités compétentes.[38] À la demande de l'autorité compétente luxembourgeoise, le point de contact unique doit transmettre les notifications d'opérateurs de services essentiels aux points de contact uniques des autres Etats membres touchés par l'incident. Remarquons que la Commission publiera une liste recensant les points de contact uniques des différents Etats membres.[39]

Au Luxembourg, le rôle du point de contact unique sera assuré par l'ILR, puisque cette tâche s'alignera avec ses obligations d'autorité compétente.

Un nouvel arrêté grand-ducal définira les missions et attributions du CERT Gouvernemental. Cet arrêté remplacera l'arrêté grand-ducal modifié du 30 juillet 2013 déterminant l'organisation et les attributions du Centre gouvernemental de traitement des urgences informatiques, aussi dénommé « Computer Emergency Response Team Gouvernemental ».[40]

Ad article 2

Conformément à la directive NIS, les obligations qui incombent aux OSE et aux FSN ne s'appliquent pas aux entreprises qui fournissent des réseaux de communications publics ou des services de communications électroniques accessibles au public au sens de la loi modifiée du 27 février 2011 sur les réseaux et les services de communications électroniques, vu qu'elles sont soumises aux exigences particulières relatives à la sécurité et à l'intégrité des réseaux et services.[41] Toutefois, si une telle

---

36 Consid. (17) Directive NIS.

37 Consid. (17) Directive NIS.

38 Art. 10 Directive NIS.

39 Art. 8, paragraphe 7 Directive NIS.

40 *Mém. A* n° 161, 6 septembre 2013, p. 3092.

41 Art. 45 et s., loi modifiée du 27 février 2011 sur les réseaux et les services de communications électroniques, *Mém. A* n° 43, 8 mars 2011, p. 610.

entreprise fournit également d'autres services tels que des services numériques (par exemple un service informatique en nuage ou un service de place de marché en ligne) ou des services tels que le DNS ou l'IXP, elle sera soumise aux exigences de sécurité et de notification prévues par la présente loi pour la fourniture de ces services particuliers, si les conditions de l'article 6 sont réunies.

L'article 2, paragraphe 1er, précise en outre que les exigences en matière de sécurité et de notification prévues par la directive ne s'appliquent pas non plus aux prestataires de services de confiance qui sont soumis à des exigences similaires en vertu de l'article 19 du règlement (UE) nº 910/2014.

Le deuxième paragraphe de l'article 2 traite des OSE et des FSN qui opèrent dans des secteurs de l'économie qui sont déjà réglementés ou le seront à l'avenir par des actes juridiques nationaux ou européens comportant des règles relatives à la sécurité des réseaux et des systèmes d'information. Si ces actes juridiques sectoriels contiennent des dispositions imposant des exigences relatives à la sécurité des réseaux et des systèmes d'information ou à la notification des incidents et que ces exigences ont un effet au moins équivalent à celui des obligations figurant dans la présente loi, ces dispositions spéciales devraient prévaloir sur les dispositions générales énoncées dans la loi NIS. Lorsque des actes juridiques sectoriels s'appliquent, la procédure d'identification des OSE ne sera pas mise en œuvre.[42] Il est à noter que les Etats membres doivent fournir à la Commission des informations sur l'application de telles dispositions de *lex specialis*.[43]

En ce qui concerne les OSE, on retrouve des législations spéciales dans des secteurs spécifiques. Ainsi, la réglementation et la surveillance dans les secteurs de la banque et des infrastructures des marchés financiers sont hautement harmonisées au niveau de l'Union au moyen de dispositions du droit primaire et du droit dérivé de l'Union et de normes élaborées en collaboration avec les autorités européennes de surveillance.[44] D'un côté, ces règles visent à assurer la sécurité, l'intégrité et la résilience des réseaux et des systèmes d'information et de l'autre, des obligations en matière de notification des incidents font partie des pratiques de surveillance normales dans le secteur financier et sont souvent incluses dans les manuels de surveillance.[45]

Exemples de *lex specialis* dans les secteurs de la banque et des infrastructures des marchés financiers :

– Selon la Commission, les exigences en matière de sécurité et de notification imposées aux prestataires de services de paiement dans la directive (UE) 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015 concernant les services de paiement dans le marché intérieur, modifiant les directives 2002/65/CE, 2009/110/CE et 2013/36/UE et le règlement (UE) no 1093/2010, et abrogeant la directive 2007/64/CE[46] (« directive sur les services de paiement 2 ») seraient à considérer comme ayant un effet au moins équivalent à celui des dispositions de la directive NIS.[47]
– De même, dans le secteur des infrastructures des marchés financiers, les contreparties centrales sont, par le biais du règlement (UE) n° 648/2012 du Parlement européen et du Conseil du 4 juillet 2012 sur les produits dérivés de gré à gré, les contreparties centrales et les référentiels centraux[48] et le règlement délégué (UE) n° 153/2013 de la Commission du 19 décembre 2012 complétant le règlement (UE) n° 648/2012 du Parlement européen et du Conseil en ce qui concerne les normes techniques de réglementation régissant les exigences applicables aux contreparties centrales[49] soumises à des obligations de sécurité pouvant être considérées comme équivalentes à celles énoncées par la directive NIS.[50] Or, puisque ces actes juridiques ne prescrivent pas d'obligation de notification, les contreparties centrales resteraient soumises aux obligations de notifications imposées par la directive NIS.[51]

---

42 Voir les explications sous l'article 6.

43 Consid. (9) Directive NIS.

44 Consid. (12) Directive NIS.

45 Consid. (13) Directive NIS.

46 *J.O.U.E.*, L 337 du 23 décembre 2015, p. 35.

47 Annexe de la communication de la Commission au Parlement européen et au Conseil, *o.c.*, (v. note 19), p. 39.

48 *J.O.U.E.*, L 201 du 27 juillet 2012, p. 1.

49 *J.O.U.E.*, L 52 du 23 février 2013, p. 41.

50 Annexe de la communication de la Commission au Parlement européen et au Conseil, *o.c.*, (v. note 19), p. 39.

51 Cooperation Group Working Document, « Sector-specific Union legal acts in the context of Article 1(7) of Directive (EU) 2016/1148 of the European Parliament and the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union ».

– Finalement, la directive 2014/65/UE du Parlement européen et du Conseil du 15 mai 2014 concernant les marchés d'instruments financiers et modifiant la directive 2002/92/CE et la directive 2011/61/UE[52] et le règlement délégué (UE) 2017/584 de la Commission du 14 juillet 2016 complétant la directive 2014/65/UE du Parlement européen et du Conseil par des normes techniques de réglementation précisant les exigences organisationnelles applicables aux plateformes de négociation[53] imposent des obligations de sécurité aux plateformes de négociation qui sont équivalentes à celles dictées par la directive NIS. Néanmoins, le règlement délégué limite l'obligation de notification aux incidents provoqués par une utilisation abusive ou un accès non autorisé[54] et ainsi, les dispositions en matière de notification de ce règlement délégué ne peuvent être considérées comme au moins équivalentes à celles énoncées dans la directive NIS.

Notons qu'au niveau des FSN, aucune législation sectorielle spécifique ne prévoit des exigences de sécurité et de notification comparables à celles énoncées à l'article 10 de la loi NIS, qui pourraient être prises en considération dans l'application de l'article 2, paragraphe 2, de la loi.[55]

Ad article 3

En application de l'article 108*bis* de la Constitution, cet article permet à l'ILR et à la CSSF de prendre des règlements dans le contexte des nouvelles missions leurs attribuées en vertu de la présente loi.

Ad article 4

Alors que les nouvelles missions de la CSSF en tant qu'autorité compétente se recoupent largement avec le domaine de compétence actuel de la CSSF, l'ILR voit ses compétences élargies de par ses nouvelles attributions en tant qu'autorité compétente et point de contact national unique. De ce fait, l'ILR se voit accorder une contribution financière destinée à compenser les frais engendrés par les nouvelles tâches se situant dans des secteurs qui, à présent, ne relèvent pas de la compétence de l'ILR.

Ad article 5

Comme mentionné *supra* sous l'article 1er, le rôle de l'ILR en tant que point de contact unique se situe dans le domaine de la coordination des tâches liées à la sécurité des réseaux et des systèmes d'information et de la coopération transfrontalière avec les autorités compétentes des autres Etats membres, ainsi qu'avec le groupe de coopération et le réseau des CSIRT.

Ad article 6

L'article 6 décrit le processus d'identification des opérateurs de services essentiels. En effet, il revient aux autorités compétentes d'établir quelles entités remplissent les critères de la définition d'un opérateur de services essentiels et d'informer les OSE ainsi identifiés qu'ils tombent sous le champ d'application de la présente loi.

La Commission recommande de réaliser cette démarche d'identification en six étapes :[56]

1. L'entité appartient-elle à un secteur/sous-secteur et correspond-elle au type visé à l'annexe de la loi ?

   L'autorité nationale compétente devrait évaluer si une entité établie sur le territoire luxembourgeois appartient aux secteurs et sous-secteurs visés en annexe. L'annexe reprend les secteurs, sous-secteurs et types d'entités énoncés dans la directive et sont considérés comme essentiels au bon fonctionnement du marché intérieur. En particulier, l'annexe se réfère aux secteurs et sous-secteurs suivants :

   – Energie : électricité, pétrole et gaz ;
   – Transports : transport aérien, transport ferroviaire, transport par voie d'eau, transport routier ;
   – Banques ;

52 *J.O.U.E.*, L 173 du 12 juin 2014, p. 349.

53 *J.O.U.E.*, L 87 du 31 mars 2017, p. 350.

54 Art. 23(3).

55 Annexe de la communication de la Commission au Parlement européen et au Conseil, *o.c.*, (v. note 19), p. 38.

56 *Ibid.*, p. 26 et s.

- Infrastructures de marchés financiers ;
- Secteur de la santé ;
- Fourniture et distribution d'eau potable ;
- Infrastructures numériques : IXP, fournisseurs de services DNS, registres de noms de domaines de haut niveau.

La décision d'identification sera notifiée à l'OSE. Cette notification relève du droit commun de la procédure administrative non contentieuse et n'est soumise à aucune exigence de forme particulière. La preuve de la notification incombera à l'autorité compétente concernée à l'origine de la notification.

2. Une *lex specialis* est-elle applicable ?

Dans une deuxième étape, il est à vérifier si l'entité est soumise à une *lex specialis* et, dans l'affirmative, si celle-ci prévoit des obligations au moins équivalents à celles énoncées dans la loi NIS.[57] Si une telle *lex specialis* existe, l'autorité compétente concernée ne devra pas poursuivre la procédure d'identification.

3. L'opérateur fournit-il un service essentiel au sens de la loi ?

En vertu de l'article 6, paragraphe 1er, point 1., l'entité soumise à l'identification doit fournir un service qui est essentiel au maintien d'activités sociétales et/ou économiques critiques. En faisant cette analyse, l'autorité compétente concernée devra tenir compte du fait qu'une seule entité peut fournir à la fois des services essentiels et non essentiels. Ainsi, dans le secteur du transport aérien, les aéroports fournissent des services qui pourraient être considérés comme essentiels, tels que la gestion des pistes, mais aussi un certain nombre de services qui pourraient être considérés comme non essentiels, tels que la mise à disposition de zones commerciales. Les OSE ne devraient être soumis aux exigences de sécurité spécifiques que pour les services qui sont jugés essentiels.[58]

Remarquons qu'en vertu de l'article 6, paragraphe 3, les autorités compétentes établiront une liste des services qui sont considérés comme essentiels.

4. Le service est-il tributaire d'un réseau et d'un système d'information ?

Dans une prochaine étape, l'autorité compétente concernée devra évaluer si l'entité fournit un service qui est tributaire des réseaux et des systèmes d'information (article 6, paragraphe 1er, point 2).

5. Un incident de sécurité aurait-il un effet disruptif important ?

Ensuite, en vertu de l'article 6, paragraphe 1er, point 3., l'autorité compétente concernée évaluera si un incident aurait un effet disruptif important sur la fourniture de son service essentiel. Cet effet disruptif est évalué sur base de facteurs transsectoriels et sectoriels, énumérés de manière non limitative à l'article 6, paragraphe 2 :

- le nombre d'utilisateurs tributaires du service fourni par l'entité concernée. Selon le groupe de travail NIS, sont à considérer comme « utilisateurs » les personnes physiques et morales ayant conclu un contrat de fourniture de services avec l'opérateur ;[59]
- la dépendance des autres secteurs visés en annexe à l'égard du service fourni par cette entité. En d'autres mots, il faudra évaluer le degré de dépendance d'autres OSE du service essentiel fourni par un OSE en particulier ;[60]
- les conséquences que des incidents pourraient avoir, en termes de degré et de durée, sur les fonctions économiques ou sociétales ou sur la sûreté publique ;
- la part de marché de cette entité ;
- la portée géographique eu égard à la zone susceptible d'être touchée par un incident. La zone géographique vise les Etats membres ou régions au sein de l'Union européenne affectés par la défaillance du service essentiel ;[61]

---

57 Il est renvoyé aux développements sous l'article 2, paragraphe 2.

58 Consid. (22) Directive NIS.

59 Cooperation Group, Working Group 3, « Reference Document on Incident Notification for Operators of Essential Services » (9.11.2017), p. 18.

60 *Ibid.*, p. 20.

61 *Ibid.*, p. 19.

– l'importance que revêt l'entité pour garantir un niveau de service suffisant, compte tenu de la disponibilité de solutions de rechange pour la fourniture de ce service.

Les facteurs sectoriels évoqués à l'article 6, paragraphe 2, pourraient inclure pour les fournisseurs d'énergie, le volume ou la proportion d'énergie produite au niveau national ; pour les fournisseurs de pétrole, le volume journalier ; pour le transport aérien, y compris les aéroports et les transporteurs aériens, le transport ferroviaire et les ports maritimes, la proportion du volume de trafic national et le nombre de passagers ou d'opérations de fret par an ; pour les infrastructures bancaires ou des marchés financiers, leur importance systémique sur la base de leurs actifs totaux ou du ratio entre ces actifs totaux et le PIB ; pour le secteur de la santé, le nombre annuel de patients pris en charge par le prestataire ; pour la production, le traitement et la distribution d'eau, le volume d'eau, le nombre et les types d'utilisateurs servis, y compris, par exemple, des hôpitaux, des organismes de service public ou des particuliers, ainsi que l'existence d'autres sources d'approvisionnement en eau couvrant la même zone géographique.[62]

6. L'opérateur concerné fournit-il des services essentiels dans d'autres Etats membres ?

Finalement, lorsqu'un opérateur fournit ses services essentiels dans plusieurs Etats membres, les autres Etats membres concernés devront être consultés (article 6, paragraphe 4).

Ad article 7

Puisque les OSE jouent un rôle important pour la société et l'économie, ils sont tenus de prendre les mesures de sécurité appropriées afin de protéger leurs réseaux et systèmes d'information. Dans ce sens, cette nouvelle législation entend promouvoir une culture de gestion des risques, qui implique d'un côté l'analyse des risques et de l'autre, l'application de mesures de sécurité adaptées aux risques encourus.[63]

Notons que la loi fait reposer la responsabilité de garantir la sécurité des réseaux et des systèmes d'information sur les opérateurs de services essentiels et ce même dans les cas où la gestion de la sécurité ou la maintenance des réseaux auraient été sous-traitées.[64] Cette approche est en enclin avec la législation dans le secteur des télécommunications où une culture de gestion des risques s'est établie au fil des années. Ainsi, il revient aux entreprises fournissant des réseaux de communications publics ou des services de communications électroniques accessibles au public de prendre les mesures techniques et organisationnelles adéquates afin de gérer les risques en matière de sécurité des réseaux et des services de manière appropriée.[65]

Afin d'identifier les risques, les OSE utilisent un cadre d'analyse des risques approprié pouvant être précisé par l'autorité compétente concernée, notamment par voie de règlement. Cette phrase a été rajoutée par rapport à la directive NIS, pour pouvoir demander aux OSE d'utiliser un outil d'analyse de risque spécifique, à l'instar de la pratique que l'ILR a établi dans le secteur des télécommunications.[66]

Bien que le troisième paragraphe de l'article 7 constitue une précision par rapport au texte de la directive, il se trouve dans la lignée de l'esprit de la directive qui fait reposer un devoir de surveillance sur les épaules des Etats membres, représentés par les autorités compétentes (« Les Etats membres veillent à ce que… »). Afin que l'autorité compétente concernée puisse assurer cette mission de surveillance, il est crucial que les OSE lui notifient les mesures de gestion des risques et de prévention des incidents mises en place au sein de leur entité. Remarquons que ce nouveau paragraphe assure en

---

62 Consid. (28) Directive NIS.

63 Consid. (44) Directive NIS.

64 Consid. (52) Directive NIS.

65 Art. 45, paragraphe 2, de la loi modifiée du 27 février 2011 sur les réseaux et les services de communications électroniques (v. note 41).

66 Art. 45 de la loi modifiée du 27 février 2011 sur les réseaux et les services de communications électroniques (v. note 41) ; art. 2 du règlement 15/200/ILR du 18 décembre 2015 portant sur les modalités de notification des mesures de sécurité à prendre par les entreprises fournissant des réseaux de communications publics et/ou des services de communications électroniques au public dans le cadre de l'article 45 (1) et (2) de la loi du 27 février 2011 sur les réseaux et les services de communications électroniques, Mém. A, n° 261, 29 décembre 2015, p. 6287.

outre un parallélisme avec la législation en matière de télécommunications qui exige une notification similaire à l'ILR.[67]

Conformément à l'article 7, paragraphe 4, les OSE doivent notifier les incidents qui ont un impact significatif sur la continuité des services essentiels qu'ils fournissent. Ainsi, tout évènement ayant un impact négatif non seulement sur la disponibilité, mais aussi sur l'authenticité, l'intégrité ou la confidentialité des données ou des services connexes pourrait déclencher l'obligation de notification. En effet, la continuité du service telle que visée à l'article article 7, paragraphe 4, peut être compromise non seulement dans les cas où la disponibilité matérielle est en jeu, mais aussi par tout autre incident de sécurité affectant la bonne fourniture du service.[68]

Puisque la directive laisse aux Etats membres le choix de définir si les OSE notifient ces incidents à l'autorité compétente ou au CSIRT (*Computer Security Incident Response Team*), les auteurs du présent projet de loi ont pris l'option que les OSE ne notifient, pour des raisons de simplification administrative, qu'à la seule autorité compétente concernée et que cette notification soit par la suite transmise au CERT Gouvernemental ou au CIRCL, en fonction de leurs compétences respectives. Tandis que le CERT Gouvernemental est l'entité gestionnaire d'incidents du réseau étatique,[69] le CIRCL assure ce rôle au niveau du secteur privé. Notons que l'article 16 de la loi modifiée du 23 décembre 1998 portant création d'une commission de surveillance du secteur financer[70] ne fait pas obstacle à cette communication.

Les régulateurs entendent profiter de la période courant jusqu'à l'adoption du présent projet de loi afin d'examiner la possibilité de mettre en place une plateforme de notification unique, de sorte que les opérateurs de services essentiels et les fournisseurs de service numérique qui auraient des obligations de notification sous d'autres législations ne devraient faire qu'une seule notification. En outre, il serait évité que l'OSE ou le FSN transmette la notification à une autorité non compétente. Cette plateforme de notification unique pourrait être mise à profit pour transmettre la notification au CERT Gouvernemental, respectivement CIRCL.

Vu que seuls les incidents ayant un impact significatif devront être notifiés à l'autorité compétente concernée, il est impératif de pouvoir déterminer l'importance de l'impact. Cette ampleur pourra être déterminée à l'aide de paramètres définis au paragraphe 5 du même article :

– le nombre d'utilisateurs touchés par la perturbation du service essentiel ;[71]
– la durée de l'incident. Selon le groupe de travail NIS, la durée commence à partir du moment où le service essentiel offert par l'opérateur est perturbé par un incident affectant la confidentialité, l'intégrité, la disponibilité ou l'authenticité des systèmes informatiques garantissant le service essentiel ;[72]
– la portée géographique eu égard à la zone touchée par l'incident.[73]

S'il s'avère que l'incident survenu au Luxembourg pourrait affecter les services essentiels fournis dans d'autres Etats membres, l'autorité compétente concernée en avertit l'autorité compétente des Etats membres concernés. L'article 16 de la loi modifiée du 23 décembre 1998 portant création d'une commission de surveillance du secteur financer ne fait pas obstacle à cette communication. Sur demande de l'autorité compétente concernée, cette notification sera transmise par le point de contact luxembourgeois aux points de contact des Etats concernés.

Pour assurer l'information effective des Etats membres et de la Commission sur les notifications reçues par les différentes autorités compétentes à travers l'Union, la directive NIS prescrit que le point de contact unique soumette annuellement un rapport de synthèse au groupe de coopération. Afin que

---

67 Article 45, paragraphe 3, de la loi modifiée du 27 février 2011 sur les réseaux et les services de communications électroniques (v. note 41).

68 Annexe de la communication de la Commission au Parlement européen et au Conseil, *o.c.*, (v. note 20), p. 32.

69 Arrêté grand-ducal du 30 juillet 2013 déterminant l'organisation et les attributions du Centre gouvernemental de traitement des urgences informatiques, aussi dénommé « Computer Emergency Response Team Gouvernemental », *Mém. A* n° 161, 6 septembre 2013, p. 3092.

70 *Mém. A* n° 112, 24 décembre 1998, p. 2985.

71 Voir commentaire de l'article 6.

72 Cooperation Group, Working Group 3, *o.c.*, (v. note 59), p. 19.

73 Voir commentaire de l'article 6.

le point de contact luxembourgeois puisse assurer cette responsabilité, il faut qu'il dispose des informations nécessaires de la part des autorités compétentes (article 7, paragraphe 7).

Remarquons que le rapport de synthèse transmis au groupe de coopération sera rendu anonyme afin de préserver la confidentialité des notifications et l'identité des OSE et FSN. En effet, les données relatives à l'identité des entités qui sont à l'origine de la notification ne sont pas requises pour l'échange de bonnes pratiques au sein du groupe de coopération.[74]

Finalement, l'article 7, paragraphe 8, prévoit que le public peut être sensibilisé aux incidents qu'un OSE aurait pu connaître. Or, cette divulgation d'informations sur les incidents signalés aux autorités compétentes devrait être le reflet d'un compromis entre l'intérêt du public d'être informé des menaces et des éventuelles conséquences néfastes et l'intérêt des entités de préserver leur image et leur position sur le marché. En outre, en mettant en œuvre l'obligation de notification, l'autorité compétente concernée devrait être particulièrement attentive à la nécessité de garantir la stricte confidentialité des informations sur les vulnérabilités des produits avant la publication des mises à jour de sécurité appropriées.[75]

Ad article 8

Afin de garantir que les autorités compétentes puissent contrôler et, le cas échéant, faire respecter les obligations énoncées dans la présente loi, l'article 8 leur confère des pouvoirs contraignants. Ainsi, elles peuvent demander aux OSE de leur fournir des informations supplémentaires nécessaires pour évaluer la sécurité de leurs réseaux et systèmes d'information, ainsi que des éléments prouvant la mise en œuvre effective des politiques de sécurité. Sur ce dernier point, l'article 8, paragraphe 1er, point 2., va plus loin que la directive en autorisant l'autorité compétente concernée de charger un auditeur externe pour contrôler la mise en œuvre effective de la politique de sécurité de l'OSE. Ce pouvoir a été rajouté afin de conférer les mêmes pouvoirs aux autorités compétentes sous la directive NIS que ceux dont l'ILR dispose dans le secteur des télécommunications.[76]

En outre, le texte de la loi diverge du texte de la directive en ce qu'elle permet aux autorités compétentes d'exiger que les informations soient fournies dans un certain délai et qu'elles respectent un niveau de détail prédéfini. Ici aussi, il s'agit de garantir un parallélisme avec la législation sur les télécommunications.[77]

Après que les autorités compétentes aient reçu les informations susmentionnées, elles peuvent donner des instructions contraignantes aux OSE, afin que ceux-ci se conforment aux obligations leur incombant sous cette loi.

Finalement, l'article 8, paragraphe 3, transposant l'article 15, paragraphe 3 de la directive NIS, prévoit que l'autorité compétente concernée coopère avec la Commission nationale pour la protection des données pour tous les incidents qui ont donné lieu à une violation des données à caractère personnel.

Ad article 9

Compte tenu du caractère transfrontalier des FSN, il est important de de fixer le champ de compétence des autorités compétentes à travers l'Union. La directive NIS ne suit pas le modèle des juridictions parallèles multiples, mais une approche fondée sur le critère de l'établissement principal du fournisseur de service numérique. Ainsi, relèvent de la compétence des autorités luxembourgeoises, les FSN ayant leur établissement principal au Grand-Duché. En principe, l'établissement principal correspond à l'endroit où le FSN a son siège social. Les considérants de la directive précisent en outre que l'établissement suppose l'exercice réel et effectif d'une activité au moyen d'une installation stable et que la forme juridique de l'établissement (succursale, filiale ou autre) n'est pas déterminante à cet égard. Or, il faut noter que la présence physique des réseaux et systèmes d'information sur le territoire d'un Etat

---

74 Consid. (33) Directive NIS.

75 Consid. (59) Directive NIS.

76 Article 46, paragraphe 3, de la loi modifiée du 27 février 2011 sur les réseaux et les services de communications électroniques (v. note 41).

77 Article 14, alinéa 3, de la loi modifiée du 27 février 2011 sur les réseaux et les services de communications électroniques (v. note 41).

membre ne permettent pas à eux seuls de conclure que l'établissement principal d'un fournisseur se situe dans cet Etat membre.[78]

Lorsqu'un fournisseur de service numérique, qui n'est pas établi dans l'Union, propose des services à l'intérieur de l'Union, il doit désigner un représentant dans l'un des Etats membres dans lesquels il offre ses services. Le représentant établi au Luxembourg a pour mission d'agir pour le compte du FSN et pourra ainsi être contacté par les autorités compétentes luxembourgeoises.

Conformément à l'article 9, paragraphe 2, les FSN qui sont des microentreprises ou des petites entreprises au sens de du règlement grand-ducal du 16 mars 2005 portant adaptation de la définition des micro, petites et moyennes entreprises, ne devront pas respecter les exigences en matière de sécurité et de notification visées à l'article 10. Ainsi, les entreprises qui occupent moins de 50 personnes et dont le chiffre d'affaires annuel ou le total du bilan annuel n'excède pas 10 millions d'euros ne sont pas liées par ces obligations.

Ad article 10

Comme pour les OSE, la directive entend promouvoir une culture de gestion des risques en imposant aux FSN de garantir la sécurité de leurs réseaux et de leurs systèmes d'information. La hauteur de ces mesures de sécurité devrait être proportionnée à la hauteur du risque que présentent les réseaux et systèmes d'information concernés. Dans la pratique, le degré de risque auquel doivent faire face les FSN est souvent moins élevé que le degré de risque auquel doivent répondre les OSE, de par leur définition cruciaux pour le maintien de fonctions sociétales et économiques critiques. Par conséquent, les exigences en matière de sécurité imposées aux FSN pourraient être moins strictes que celles prescrites aux OSE.[79]

Selon l'article 10, paragraphe 1er, alinéa 2, les éléments à prendre en considération par les FSN pour gérer les risques qui menacent la sécurité des réseaux et des systèmes d'information sont précisés dans le règlement d'exécution 2018/151 de la Commission européenne.[80]

Remarquons que, contrairement aux OSE, les FSN ne font pas l'objet d'une identification par les autorités compétentes. Par conséquent, les obligations dictées par la loi aux FSN en matière de sécurité et de notification s'appliquent automatiquement à tous les FSN relevant de son champ de compétence, sans qu'une intervention préalable de l'autorité compétente ne soit nécessaire.[81] En outre, les considérants de la directive posent que les FSN devraient faire l'objet d'une surveillance a posteriori allégée et réactive. L'autorité compétente concernée ne devrait dès lors intervenir que lorsqu'elle est informée, par exemple par le FSN lui-même, par une autre autorité compétente, y compris une autorité compétente d'un autre Etat membre, ou par un utilisateur du service, d'éléments selon lesquels un FSN ne satisfait pas aux exigences de la présente loi, notamment à la suite de la survenance d'un incident. L'autorité compétente concernée n'a dès lors pas une obligation générale de surveiller les fournisseurs de service numérique.[82]

Selon l'article 10, paragraphe 3, les FSN sont tenus de notifier à l'autorité compétente concernée les incidents graves ayant un impact significatif sur la fourniture du service. Afin de déterminer l'ampleur de l'impact, l'article 10, paragraphe 4, fournit cinq paramètres :

– le nombre d'utilisateurs touchés par l'incident, en particulier ceux qui recourent au service pour la fourniture de leurs propres services ;
– la durée de l'incident ;
– la portée géographique eu égard à la zone touchée par l'incident ;
– la gravité de la perturbation du fonctionnement du service ;
– l'ampleur de l'impact sur les fonctions économiques et sociétales.

---

78 Consid. (64) Directive NIS.

79 Consid. (49) Directive NIS.

80 Règlement d'exécution (UE) 2018/151 de la Commission du 30 janvier 2018 portant modalités d'application de la directive (UE) 2016/1148 du Parlement européen et du Conseil précisant les éléments à prendre en considération par les fournisseurs de service numérique pour gérer les risques qui menacent la sécurité des réseaux et des systèmes d'information ainsi que les paramètres permettant de déterminer si un incident a un impact significatif, *J.O.U.E.* L 26 du 31 janvier 2018, p. 48.

81 Consid. (57) Directive NIS.

82 Consid. (60) Directive NIS.

Ces paramètres seront précisés par le règlement d'exécution 2018/151 de la Commission.[83]

Comme expliqué pour les OSE sous l'article 7, paragraphe 6, il est envisagé de mettre en place une plateforme de notification unique, destinée à répartir les notifications d'incidents à l'autorité compétente concernée, respectivement au GovCERT ou CIRCL.

Les paragraphes 5 et 6 de l'article 10 transposent fidèlement la directive NIS et ne suscitent pas de remarque particulière.

Remarquons que l'article 16 de la loi modifiée du 23 décembre 1998 portant création d'une commission de surveillance du secteur financer ne fait pas obstacle aux notifications prévues à l'article 10, paragraphes 3 et 6.

En ce qui concerne le rapport de synthèse prescrit par l'article 10, paragraphe 7, et la divulgation d'informations au public décrite au paragraphe 8 du même article, il est renvoyé aux développement sous l'article 7, paragraphes 7 et 8.

Ad article 11

Puisque les FSN sont soumis à un contrôle a posteriori, il est d'autant plus important que ce contrôle soit efficient. Ainsi, l'autorité compétente concernée dispose du pouvoir d'imposer aux FSN de lui communiquer les informations nécessaires pour évaluer la sécurité de leurs réseaux et systèmes d'information et de leur imposer de corriger les manquements aux obligations de sécurité et de notification.

Lorsque l'autorité compétente concernée met en œuvre les mesures prévues par l'article 11, elle veille à coopérer avec les Etats membres dans lesquels pourraient être situés les réseaux et systèmes d'information. Cette assistance et coopération peut prendre la forme d'un simple échange d'informations entre autorités compétentes concernées ou d'une demande de prise de mesures visées à l'article 11, paragraphe 1er.

Ad article 12

Les entités qui ne relèvent pas du champ d'application de la présente loi peuvent connaître des incidents ayant des conséquences importantes sur les services qu'elles fournissent. Lorsque ces entités estiment qu'il est dans l'intérêt public de notifier la survenance de tels incidents, elles seront en mesure de le faire à titre volontaire. Ces notifications seront traitées par l'autorité compétente concernée lorsque leur traitement ne fait pas peser de charge disproportionnée ou inutile sur l'autorité concernée.[84]

Ad article 13

Afin d'éviter que la présente loi reste lettre morte, il y a lieu de prévoir des sanctions administratives à l'encontre de ceux qui ne la respectent pas. Ainsi, l'autorité compétente concernée peut décider des sanctions à l'encontre des OSE et des FSN s'ils ne se conforment pas aux articles 7, 8, 10 et 11 ou aux mesures prises en exécution de la loi NIS.

Remarquons que les sanctions administratives énumérées dans l'article 13 et la procédure y relative s'inspirent fortement de la législation existante dans les secteurs régulés par l'ILR.[85] Le maximum des amendes d'ordre est fixé à 125.000 euros.

L'étendue du paragraphe 5 se limite à l'ILR, puisque pour la CSSF, la question sera réglée par son règlement taxes.

Ad article 14

La transposition de la directive NIS s'accompagne de changements dans le paysage institutionnel des autorités étatiques en charge de la cybersécurité. Alors que l'Agence nationale de la sécurité des systèmes d'information (ANSSI) a été l'autorité compétente concernée en matière d'agrément

---

83 Règlement d'exécution (UE) 2018/151 de la Commission du 30 janvier 2018 portant modalités d'application de la directive (UE) 2016/1148 du Parlement européen et du Conseil précisant les éléments à prendre en considération par les fournisseurs de service numérique pour gérer les risques qui menacent la sécurité des réseaux et des systèmes d'information ainsi que les paramètres permettant de déterminer si un incident a un impact significatif, *J.O.U.E.* L 26 du 31 janvier 2018, p. 48.

84 Consid. (67) Directive NIS.

85 Voir notamment l'article 60 de la loi modifiée du 1er août 2007 relative à l'organisation du marché du gaz naturel et l'article 65 de la loi modifiée du 1er août 2007 relative à l'organisation du marché de l'électricité.

cryptographique,[86] il a été jugé qu'une séparation nette devrait se faire entre l'autorité qui émet les politiques de sécurité (ANSSI) et l'autorité qui veille à ce que les produits cryptographiques soient conformes à ces politiques de sécurité. Ainsi, cette loi confère la mission d'autorité d'agrément cryptographique au Centre des technologies de l'information de l'Etat (CTIE).

Ad article 15

Pour atteindre et maintenir un niveau élevé de sécurité des réseaux et des systèmes d'information, une stratégie nationale en matière de sécurité des réseaux et des systèmes d'information devra définir les objectifs stratégiques et les actions politiques concrètes à mettre en œuvre.

Vu que cette stratégie nationale en matière de sécurité des réseaux et des systèmes d'information peut être considérée comme équivalente à une stratégie nationale de cybersécurité[87] et que le Luxembourg dispose déjà d'une telle stratégie nationale en matière de cybersécurité élaborée par un comité interministériel présidé par le Haut-Commissariat à la Protection nationale (HCPN), la nouvelle loi fortifie ce rôle de coordinateur en lui accordant une assise juridique dans la loi HCPN.

Les articles 2 et 9bis rajoutés dans la loi du 23 juillet 2016 portant création d'un Haut-Commissariat à la Protection nationale constituent une transposition fidèle de la directive NIS, tandis que l'article 3 a été modifié par souci d'exhaustivité.

L'article 8 de la loi HCPN a été modifié afin de corriger une erreur matérielle.

*

TABLEAU DE CONCORDANCE

Avant-projet de loi	*Directive (UE) 2016/1148*
Article 1, 1.	Article 4, 1)
Article 1, 2.	Article 4, 2)
Article 1, 3.	Article 4, 4)
Article 1, 4.	Article 4, 5)
Article 1, 5.	Article 4, 6)
Article 1, 6.	Article 4, 7)
Article 1, 7.	Article 4, 8)
Article 1, 8.	Article 4, 9)
Article 1, 9.	Article 4, 10)
Article 1, 10.	Article 4, 11)
Article 1, 11.	Article 4, 12)
Article 1, 12.	Article 4, 13)
Article 1, 13.	Article 4, 14)
Article 1, 14.	Article 4, 15)
Article 1, 15.	Article 4, 16)
Article 1, 16.	Article 4, 17)
Article 1, 17.	Article 1, 18)
Article 1, 18.	Article 1, 19)
Article 1, 19.	Article 8, (1)

86 Arrêté grand-ducal du 10 février 2015 1. portant fixation de la gouvernance en matière de gestion de la sécurité de l'information 2. modifiant l'arrêté grand-ducal du 30 juillet 2013 déterminant l'organisation et les attributions du Centre gouvernemental de traitement des urgences informatiques, aussi dénommé «Computer Emergency Response Team Gouvernemental», *Mém. A* n° 30, 20 février 2015, p. 338.

87 Annexe de la communication de la Commission au Parlement européen et au Conseil, *o.c.*, (v. note 19), p. 5.

Avant-projet de loi	*Directive (UE) 2016/1148*
Article 1, 20.	Article 8, (3) et (4)
Article 1, 21.	Nouveau
Article 1, 22.	Nouveau
Article 1, 23.	Nouveau
Article 1, 24.	Article 11, (1)
Article 1, 25.	Article 12, (1)
Article 2, (1)	Article 1, (3)
Article 2, (2)	Article 1, (7)
Article 3	Nouveau
Article 4	Nouveau
Article 5	Nouveau
Article 6, (1)	Article 5, (2)
Article 6, (2)	Article 6, (1) et (2)
Article 6, (3)	Article 5, (3)
Article 6, (4)	Article 5, (4)
Article 7, (1)	Article 14, (1)
Article 7, (2)	Article 14, (2)
Article 7, (3)	Nouveau
Article 7, (4)	Article 14, (3)
Article 7, (5), alinéa 1	Article 14, (4)
Article 7, (5), alinéa 2	Article 14, (7)
Article 7, (6)	Article 14, (5)
Article 7, (7), alinéa 1	Nouveau
Article 7, (7), alinéa 2	Article 10, (3), alinéa 2
Article 7, (8)	Article 14, (6)
Article 8, (1), alinéa 1, point 1.	Article 15, (2), alinéa 1, a)
Article 8, (1), alinéa 1, point 2.	Article 15, (2), alinéa 1, b)
Article 8, (1), alinéa 1, point 3.	Nouveau
Article 8, (1), alinéa 2	Nouveau
Article 8, (1), alinéa 3	Article 15, (2), alinéa 2
Article 8, (2)	Article 15, (3)
Article 8, (3)	Article 15, (4)
Article 9, (1), alinéa 1	Article 18, (1) et (2)
Article 9, (1), alinéa 2	Article 4, 10)
Article 9, (1), alinéa 3	Article 18, (3)
Article 9, (2)	Article 16, (11)
Article 10, (1)	Article 16, (1)
Article 10, (2)	Article 16, (2)
Article 10, (3)	Article 16, (3)
Article 10, (4), alinéa 1	Article 16, (4), alinéa 1
Article 10, (4), alinéa 2	Article 16, (4), alinéa 2
Article 10, (4), alinéa 3	Nouveau

Avant-projet de loi	*Directive (UE) 2016/1148*
Article 10, (5)	Article 16, (5)
Article 10, (6)	Article 16, (6)
Article 10, (7), alinéa 1	Nouveau
Article 10, (7), alinéa 2	Article 10, (3), alinéa 2
Article 10, (8)	Article 16, (7)
Article 11, (1), point 1.	Article 17, (2), a)
Article 11, (1), point 2.	Article 17, (2), b)
Article 11, (1), point 3.	Nouveau
Article 11, (2)	Article 17, (3)
Article 12, (1)	Article 20, (1)
Article 12, (2)	Article 20, (2)
Article 13, (1)	Article 21
Article 13, (2)	
Article 13, (3)	
Article 13, (4)	
Article 13, (5)	
Article 14	Nouveau
Article 15, (1)	Article 4, 3)
Article 15, (2)	Nouveau
Article 15, (3)	Nouveau
Article 15, (4)	Article 7, (1)
Article 16	Nouveau
Annexe	Annexe II

Directive (UE) 2016/1148	*Avant-projet de loi*
Article 1, (1)	–
Article 1, (2)	–
Article 1, (3)	Article 2, (1)
Article 1, (4)	–
Article 1, (5)	–
Article 1, (6)	–
Article 1, (7)	Article 2, (2)
Article 2, (1)	–
Article 2, (2)	–
Article 3	–
Article 4, 1)	Article 1, 1.
Article 4, 2)	Article 1, 2.
Article 4, 3)	Article 15, (1)
Article 4, 4)	Article 1, 3.
Article 4, 5)	Article 1, 4.
Article 4, 6)	Article 1, 5.
Article 4, 7)	Article 1, 6.

Directive (UE) 2016/1148	*Avant-projet de loi*
Article 4, 8)	Article 1, 7.
Article 4, 9)	Article 1, 8.
Article 4, 10)	Article 1, 9. et article 9, (1), alinéa 2
Article 4, 11)	Article 1, 10.
Article 4, 12)	Article 1, 11.
Article 4, 13)	Article 1, 12.
Article 4, 14)	Article 1, 13.
Article 4, 15)	Article 1, 14.
Article 4, 16)	Article 1, 15.
Article 4, 17)	Article 1, 16.
Article 4, 18)	Article 1, 17.
Article 4, 19)	Article 1, 18.
Article 5, (1)	–
Article 5, (2)	Article 6, (1)
Article 5, (3)	Article 6, (3)
Article 5, (4)	Article 6, (4)
Article 5, (5)	–
Article 5, (6)	–
Article 5, (7)	–
Article 6, (1)	Article 6, (2)
Article 6, (2)	Article 6, (2)
Article 7, (1)	Article 15, (4)
Article 7, (2)	–
Article 7, (3)	–
Article 8, (1)	Article 1, 19.
Article 8, (2)	–
Article 8, (3)	Article 1, 20.
Article 8, (4)	Article 1, 20.
Article 8, (5)	–
Article 8, (6)	–
Article 8, (7)	–
Article 9, (1)	–
Article 9, (2)	–
Article 9, (3)	–
Article 9, (4)	–
Article 9, (5)	–
Article 10, (1)	–
Article 10, (2)	–
Article 10, (3)	–
Article 11, (1)	Article 1, 24.
Article 11, (2)	–

Directive (UE) 2016/1148	*Avant-projet de loi*
Article 11, (3)	–
Article 11, (4)	–
Article 11, (5)	–
Article 12, (1)	Article 1, 25.
Article 12, (2)	–
Article 12, (3)	–
Article 12, (4)	–
Article 12, (5)	–
Article 13	–
Article 14, (1)	Article 7, (1)
Article 14, (2)	Article 7, (2)
Article 14, (3)	Article 7, (4)
Article 14, (4)	Article 7, (5), alinéa 1
Article 14, (5)	Article 7, (6)
Article 14, (6)	Article 7, (8)
Article 14, (7)	Article 7, (5), alinéa 2
Article 15, (1)	–
Article 15, (2)	Article 8, (1)
Article 15, (3)	Article 8, (2)
Article 15, (4)	Article 8, (3)
Article 16, (1)	Article 10, (1)
Article 16, (2)	Article 10, (2)
Article 16, (3)	Article 10, (3)
Article 16, (4), alinéa 1	Article 10, (4), alinéa 1
Article 16, (4), alinéa 2	Article 10, (4), alinéa 2
Article 16, (5)	Article 10, (5)
Article 16, (6)	Article 10, (6)
Article 16, (7)	Article 10, (8)
Article 16, (8)	–
Article 16, (9)	–
Article 16, (10)	–
Article 16, (11)	Article 9, (2)
Article 17, (1)	–
Article 17, (2)	Article 11, (1)
Article 17, (3)	Article 11, (2)
Article 18, (1)	Article 9, (1), alinéa 1
Article 18, (2)	Article 9, (1), alinéa 1
Article 18, (3)	Article 9, (1), alinéa 3
Article 19, (1)	–
Article 19, (2)	–
Article 20, (1)	Article 12, (1)
Article 20, (2)	Article 12, (2)

Directive (UE) 2016/1148	*Avant-projet de loi*
Article 21	Article 13, (1) – (5)
Article 22, (1)	–
Article 22, (2)	–
Article 23, (1)	–
Article 23, (2)	–
Article 24, (1)	–
Article 24, (2)	–
Article 24, (3)	–
Article 25, (1)	–
Article 25, (2)	–
Article 26	–
Article 27	–
Annexe I	–
Annexe II	Annexe
Annexe III	Intégré dans le texte de l'APL (article 1, 4.)

*

FICHE FINANCIERE

(article 79 de la loi modifiée du 8 juin 1999 sur le Budget, la Comptabilité et la Trésorerie de l'Etat)

Les frais supplémentaires engendrés par le projet de loi sont de trois catégories :

1. les frais liés à la mise en place d'une plateforme de notification unique ;
2. les frais de mise en place d'un service chargé de l'implémentation de la directive NIS. Ce besoin en personnel est évalué à quatre agents du groupe de traitement A1 ;
3. les frais liés à l'extension de l'outil TISRIM (outil d'implémentation d'une méthode de gestion des risques) aux secteurs visés par la directive NIS, actuellement non couverts par l'ILR.

*

TEXTES COORDONNES

LOI DU 20 AVRIL 2009
portant création du Centre des technologies de l'information de l'Etat

Texte coordonné au 27 novembre 2015

Art. 1er. Il est institué un Centre des technologies de l'information de l'Etat, dénommé ci-après «le centre», qui est placé sous l'autorité du ministre ayant les technologies de l'information de l'Etat dans ses attributions, dénommé ci-après «le ministre».

Art. 2. Le centre a pour mission:

a) la promotion et l'organisation de façon rationnelle et coordonnée de l'automatisation des administrations de l'Etat notamment en ce qui concerne la collecte, la transmission et le traitement des données;

b) l'assistance des différentes administrations de l'Etat dans l'exécution des travaux courants d'informatique, ainsi que la gestion des systèmes de communication fixes et mobiles;

c) la gestion des équipements électroniques, informatiques et de sécurité appropriés à l'accomplissement de ses attributions;

d) l'administration du réseau informatique commun et de la messagerie électronique de l'Etat;

e) la sécurité de l'informatique et le respect des dispositions de la loi relative à la protection des personnes à l'égard du traitement des données à caractère personnel, dans les limites de ses attributions;

f) la production et la personnalisation de documents administratifs sécurisés et le traitement des données biométriques y relatives;

g) l'acquisition et la gestion d'équipements informatiques et bureautiques et de machines de bureau pour les administrations de l'Etat;

h) la gestion d'un centre de support destiné aux utilisateurs internes et externes des systèmes d'informations gérés par le centre;

i) l'élaboration et la tenue à jour d'une cartographie des processus des administrations de l'Etat et de leur interopérabilité;

j) le support organisationnel des administrations de l'Etat et leur accompagnement dans leurs projets de réorganisation;

k) la recherche de synergies entre les différentes administrations de l'Etat et l'optimisation de leurs échanges d'informations;

l) la coordination de la présence Internet des administrations de l'Etat;

m) la mise en place et l'exploitation des plateformes d'échange avec les citoyens et les entreprises;

n) la mise en place et l'exploitation de plateformes de collaboration reliant l'ensemble des agents de l'Etat;

o) la mise en place et la coordination d'un réseau de guichets physiques régionaux qui offrent aux citoyens un point de contact unique quelles que soient leurs démarches administratives;

p) la mise à disposition d'une base de connaissances regroupant l'ensemble des attributions de l'Etat et accessible à travers les différents canaux de services publics;

q) l'acquisition, l'entreposage et la diffusion de fournitures de bureau, de manuels et publications scolaires et d'imprimés destinés aux administrations de l'Etat;

r) l'impression, l'entreposage et la diffusion des documents parlementaires et d'ouvrages publiés par les administrations de l'Etat,

s) la transmission des informations officielles entre les gouvernements, les organismes internationaux et les administrations de l'Etat, selon les directives de sécurité en vigueur;

t) la planification, la mise en place, la gestion, l'exploitation et l'assurance de la disponibilité des systèmes de communication et d'information classifiés permettant la consultation politique et l'échange d'informations au profit du Gouvernement;

u) l'exercice, dans le cadre de ces attributions, de la fonction d'Autorité nationale de distribution, responsable de la gestion du matériel cryptographique des organismes nationaux et internationaux;

v) l'exercice de la fonction de Bureau d'ordre central qui est l'entité nationale responsable d'organiser la réception, la comptabilisation, la distribution et la destruction des pièces classifiées;

w) la mise à la disposition du Gouvernement d'une infrastructure sécurisée et des ressources administratives, logistiques, de communications électroniques et de traitement de l'information nécessaires à la gestion de crises;

x) la mise à la disposition du Gouvernement d'un centre de conférences nationales et internationales;

y) l'opération du service courrier du Gouvernement ;-

z) l'exercice, dans le cadre de ces attributions, de la fonction d'Autorité d'agrément cryptographique, chargée de veiller à ce que les produits cryptographiques soient conformes aux politiques de sécurité respectives en matière cryptographique; d'évaluer et d'agréer les produits cryptographiques pour la protection des informations classifiées jusqu'à un certain niveau de classification dans leur environnement opérationnel; de conserver et de gérer les données techniques relatives aux produits cryptographiques.

Art. 3. En outre, le centre exerce les attributions qui lui sont confiées par des dispositions légales ou Règlementaires spéciales notamment en ce qui concerne la satisfaction de besoins en informatique et en imprimés et fournitures de bureau d'utilisateurs et d'établissements autres que les administrations de l'Etat.

Art. 4. (1) Le centre est dirigé par un directeur, qui en est le chef et qui a sous ses ordres tout le personnel.

Le directeur est assisté de deux directeurs adjoints, appelés à le remplacer en cas d'absence ou en cas de vacance de poste, d'après leur rang d'ancienneté.

(2) En dehors des directeur et directeurs adjoints, le centre comprend des divisions et services dont la création et les attributions sont déterminées par règlement grand-ducal.

(3) Un règlement grand-ducal peut régler le mode de collaboration en matière informatique ainsi qu'en matière d'imprimés et de fournitures de bureau entre le centre et les administrations de l'Etat.

Art. 5. (1) Pour l'exécution des travaux informatiques confiés au centre, celui-ci bénéficie de la part des administrations de toute la collaboration nécessaire pour l'élaboration des solutions. Le centre est responsable de la conduite des travaux, sauf si les données et les spécifications des traitements mises à sa disposition ne permettent pas l'exécution correcte des travaux.

(2) Le Gouvernement en conseil détermine, sur avis du ministre, les administrations de l'Etat dotées d'un service informatique, qui peuvent assumer elles-mêmes en tout ou en partie leurs travaux d'automatisation. Pour l'exécution de ces travaux, ces administrations doivent respecter les normes de qualité et de sécurité déterminées par le centre.

Art. 6. Sont soumis à l'autorisation du ministre, l'avis du centre ayant été demandé:

a) tout projet ayant trait à l'engagement, à la formation et à la promotion du personnel informatique des services informatiques des administrations de l'Etat, pour autant que la matière informatique est concernée;

b) tout projet des administrations de l'Etat sur l'acquisition d'équipements informatiques ou sur un recours aux services ou équipements d'organismes ou d'experts informatiques extérieurs à l'administration;

c) les crédits à proposer au projet de budget annuel de l'Etat en ce qui concerne les personnel, équipements et services visés aux lettres a) et b).

Art. 7. (1) Il est créé un comité interministériel des technologies de l'information et des imprimés qui a pour mission notamment:

a) de définir les plans directeurs en matière de gouvernance électronique;

b) d'autoriser les projets d'automatisation des processus de l'administration ainsi que les projets en matière d'imprimés et d'en assurer le suivi;

c) de veiller à la création et à l'entretien dans l'administration d'un climat favorable à la réorganisation et à l'automatisation de ses processus;

d) de constituer une liaison entre le centre et les différentes administrations de l'Etat en vue de prévenir ou d'aplanir toute difficulté en rapport avec leur informatisation ou en relation avec leur gestion et leurs besoins respectifs en matière d'imprimés;

e) de conseiller, d'office ou sur demande, tant le ministre d'Etat que les ministres des ressorts respectifs et le directeur du centre sur toute question relative à la (ré)organisation et l'automatisation de l'administration;

f) de conseiller le ministre, les ministres des ressorts respectifs et le directeur du centre sur toute question en matière d'imprimés;

g) d'émettre un avis sur les contestations pouvant s'élever en matière informatique ou en matière d'imprimés entre deux ou plusieurs administrations de l'Etat ou entre une administration de l'Etat et le centre.

(2) Le comité soumet périodiquement le plan directeur en matière de gouvernance électronique pour approbation au Gouvernement en conseil.

(3) La composition et le fonctionnement du comité peuvent être déterminés par règlement grand-ducal. Le président du comité est désigné par le ministre. Le directeur du centre, ou son délégué, est d'office membre du comité.

Art. 8. (1) Les propositions élaborées par le centre concernant la solution intégrée des problèmes d'informatique communs à l'ensemble ou à certaines administrations pourront, après consultation obligatoire du comité visé à l'article 7, être déclarées par le Gouvernement en conseil d'application obligatoire pour tous les services intéressés.

(2) Les contestations pouvant s'élever en matière informatique entre deux ou plusieurs administrations de l'Etat ou entre une administration et le centre sont tranchées par le Gouvernement en conseil sur avis préalable du comité visé à l'article 7.

Art. 9. (1) Le cadre du personnel comprend un directeur, deux directeurs-adjoints et des fonctionnaires des différentes catégories de traitement telles que prévues par la loi du 25 mars 2015 fixant le régime des traitements et les conditions et modalités d'avancement des fonctionnaires de l'Etat.

(2) Le cadre prévu au présent article peut être complété par des fonctionnaires-stagiaires, des employés de l'Etat et des ouvriers de l'Etat suivant les besoins du centre et dans les limites des crédits budgétaires.

(3) Les agents du centre peuvent être placés auprès d'un département ministériel ou d'une administration de l'Etat par une décision conjointe du ministre et du ministre du ressort. Dans ce cas, et pendant toute la durée de leur placement, ils continuent de relever de l'autorité hiérarchique du directeur du centre.

(4) Sans préjudice des conditions générales d'admission au stage ainsi qu'aux examens de fin de stage et de promotion fixées par les lois et règlements, les conditions particulières d'admission au stage, de nomination et d'avancement sont déterminées par règlement grand-ducal.

Art. 10. Sont nommés par le Grand-Duc les fonctionnaires des grades supérieurs au grade 8; le ministre nomme aux autres emplois.

Le directeur et les directeurs adjoints sont nommés par le Grand-Duc sur proposition du Gouvernement en conseil.

Art. 11. (1) Une prime informatique peut être allouée aux fonctionnaires et employés travaillant à l'étude, à la conception, au développement, à l'organisation, à la réalisation, à l'exploitation ou à la maintenance de solutions informatiques.

(2) La prime est allouée sur proposition du ministre par le Gouvernement en conseil suivant des règles à établir par voie de règlement grand-ducal. Ces règles portent notamment sur la fixation de l'indemnité qui sera exprimée en points indiciaires et sur les conditions que doivent remplir les bénéficiaires. Le montant de la prime peut varier suivant des critères objectifs, tels que la fonction exercée par le fonctionnaire, le diplôme dont il est détenteur et le temps pendant lequel il travaille comme informaticien.

(3) Si un fonctionnaire ou employé a acquis une formation en informatique au cours de son service auprès de l'Etat, les frais exposés par l'Etat pour cette formation seront sujets à remboursement par le fonctionnaire ou l'employé, s'il renonce à ses fonctions au service de l'Etat ou est révoqué, après avoir bénéficié de la prime informatique.

(4) Pour l'application du paragraphe 3, le remboursement des frais de formation exposés par l'Etat est fixé à cent pour cent pour l'année en cours et l'année précédente, à soixante pour cent pour la deuxième année précédente et à trente pour cent pour la troisième année précédente. Le remboursement se fait par tranches mensuelles correspondant à dix pour cent du dernier traitement brut. Pour l'application de la règle qui précède, la prime informatique est censée comprise dans le traitement.

(5) Les dispositions du présent article sont applicables tant aux fonctionnaires et employés du centre qu'aux fonctionnaires et employés d'autres administrations de l'Etat.

Art. 12. La loi modifiée du 22 juin 1963 fixant le régime des traitements des fonctionnaires de l'Etat est modifiée comme suit:

1. A l'annexe A «Classification des fonctions», la rubrique «I. Administration générale» est complétée comme suit: au grade 16 est ajoutée la mention «Centre des technologies de l'information de l'Etat – directeur adjoint».
2. A l'annexe D, la rubrique «I. Administration générale», sous la dénomination de la carrière supérieure de l'administration; grade de computation de la bonification d'ancienneté 12, grade de début de carrière grade 16, est complétée derrière les termes de «de l'Administration de la gestion de l'eau» par la mention «du Centre des technologies de l'information de l'Etat».
3. A l'article 22, section IV, est ajoutée au premier alinéa du point 8° derrière les termes de «directeur du Service Central d'Assistance sociale» la mention «le directeur adjoint du Centre des technologies de l'information de l'Etat».

Art. 13. L'agent de l'Etat ayant été nommé à la fonction de directeur du Centre informatique de l'Etat avec effet au 1er juillet 2004 peut être chargé d'une mission particulière de planification en matière informatique auprès du ministre. Dans ce cas, il libère le poste de directeur en conservant son statut, sa rémunération ainsi que son expectative de carrière. Il peut être autorisé à porter le titre de «conseiller».

Art. 14. L'employé de l'Etat engagé le 1er septembre 2004 auprès de l'Administration gouvernementale en qualité de chargé de direction du Service eLuxembourg peut être nommé à la fonction de directeur adjoint du centre. Pour la fixation de son traitement, il conserve le niveau de grade et d'échelon atteints à la veille de l'entrée en vigueur de la présente loi, y compris la majoration d'échelon.

Art. 15. Les agents de l'Etat relevant de l'Administration gouvernementale et affectés au Service eLuxembourg au moment de l'entrée en vigueur de la présente loi sont détachés auprès du centre. Ils continuent d'avancer par référence au rang qu'ils auraient occupé dans leur cadre d'origine s'ils n'avaient pas été détachés sur base du présent article.

Art. 16. Le personnel du Centre informatique de l'Etat est repris par le Centre des technologies de l'information de l'Etat.

Art. 17. Toute référence au Centre informatique de l'Etat respectivement au Service eLuxembourg s'entend comme référence au Centre des technologies de l'information de l'Etat.

Art. 18. La loi modifiée du 29 mars 1974 créant un centre informatique de l'Etat est abrogée.

Art. 19. La présente loi entre en vigueur le premier jour du mois qui suit celui de sa publication au Mémorial.

LOI DU 23 JUILLET 2016

portant création d'un Haut-Commissariat à la Protection nationale et modifiant

a) la loi modifiée du 23 juillet 1952 concernant l'organisation militaire;

b) la loi du 8 décembre 1981 sur les réquisitions en cas de conflit armé, de crise internationale grave ou de catastrophe;

c) la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel;

d) la loi modifiée du 25 juin 2009 sur les marchés publics;

e) la loi modifiée du 9 décembre 2005 déterminant les conditions et modalités de nomination de certains fonctionnaires occupant des fonctions dirigeantes dans les administrations et services de l'État;

f) la loi modifiée du 25 mars 2015 fixant le régime des traitements et les conditions et modalités d'avancement des fonctionnaires de l'État

Chapitre 1er – *Objet*

Art. 1er. Il est créé une administration dénommée Haut-Commissariat à la Protection nationale, dont les compétences et les mécanismes selon lesquels elle intervient sont déterminés par la présente loi qui règle également l'organisation de la protection des infrastructures critiques.

Le Haut-Commissariat à la Protection nationale est placé sous l'autorité du membre du Gouvernement ayant dans ses attributions la Protection nationale.

Chapitre 2 – *Définitions*

Art. 2. Pour l'application de la présente loi, on entend par

1. «concept de protection nationale»: un concept qui consiste à prévenir les crises, respectivement à protéger le pays et la population contre les effets d'une crise. En cas de survenance d'une crise, il comprend la gestion des mesures et activités destinées à faire face à la crise et à ses effets et à favoriser le retour à l'état normal;
2. «crise»: tout évènement qui, par sa nature ou ses effets, porte préjudice aux intérêts vitaux ou aux besoins essentiels de tout ou partie du pays ou de la population, qui requiert des décisions urgentes et qui exige une coordination au niveau national des actions du Gouvernement, des administrations, des services et organismes relevant des pouvoirs publics, et, si besoin en est, également au niveau international;
3. «gestion de crises»: l'ensemble des mesures et activités que le Gouvernement initie, le cas échéant avec le concours des autorités communales concernées, pour faire face à la crise et à ses effets et pour favoriser le retour à l'état normal;
4. «infrastructure critique»: tout point, système ou partie de celui-ci qui est indispensable à la sauvegarde des intérêts vitaux ou des besoins essentiels de tout ou partie du pays ou de la population ou qui est susceptible de faire l'objet d'une menace particulière~~.~~ ;
5. «stratégie nationale en matière de sécurité des réseaux et des systèmes d'information»: un cadre prévoyant des objectifs et priorités stratégiques en matière de sécurité des réseaux et des systèmes d'information au niveau national.

Chapitre 3 – *Mission et attributions du Haut-Commissariat à la Protection nationale*

Art. 3. (1) Le Haut-Commissariat à la Protection nationale a pour mission de mettre en œuvre le concept de protection nationale tel que défini à l'article 2. Dans le cadre de cette mission, le Haut-Commissariat à la Protection nationale a pour attributions

a) quant aux mesures de prévention de crises:

1. de coordonner les contributions des ministères, administrations et services de l'État;
2. de coordonner les politiques, les projets et les programmes de recherche;
3. de procéder à l'analyse des risques et à l'organisation d'une veille;
4. de coordonner l'organisation des cours de formation et des exercices;

b) quant aux mesures d'anticipation de crises:

1. de développer et de coordonner une stratégie nationale de gestion de crises;
2. de définir la typologie, la structure, le corps et le format des plans déclinant les mesures et activités de prévention et de gestion de crises et de coordonner la planification;
3. d'initier, de coordonner et de veiller à l'exécution des activités et mesures relatives au recensement, à la désignation et à la protection des infrastructures critiques, qu'elles soient publiques ou privées;
4. de coordonner et d'élaborer une stratégie nationale en matière de sécurité des réseaux et des systèmes d'information;

c) quant aux mesures de gestion de crises:

1. d'initier, de conduire et de coordonner les tâches de gestion de crises;
2. de veiller à l'exécution de toutes les décisions prises;
3. de favoriser le plus rapidement possible le retour à l'état normal;
4. de préparer un budget commun pour la gestion de crises et de veiller à son exécution;
5. de veiller à la mise en place et au fonctionnement du Centre national de crise.

Dans le cadre de ses attributions, le Haut-Commissariat à la Protection nationale est le point de contact du Luxembourg auprès des institutions et organisations européennes et internationales et veille à une coopération efficace avec ces entités.

(2) Les autorités administratives et judiciaires, la Police grand-ducale et le Haut-Commissariat à la Protection nationale veillent à assurer une coopération efficace en matière de communication des informations susceptibles d'avoir un rapport avec leurs missions.

(3) Le Haut-Commissaire à la Protection nationale ou son délégué peuvent, par demande écrite, demander à tout détenteur d'un secret professionnel ou d'un secret protégé par une clause contractuelle la communication des informations couvertes par ce secret si la révélation dudit secret est nécessaire à l'exercice de sa mission de gestion de crises ou de protection des infrastructures critiques. Une divulgation d'informations en réponse à une telle demande n'entraîne pour l'organisme ou la personne détenteur des informations secrètes aucune responsabilité.

(4) Les informations qui sont couvertes par le secret de l'instruction relative à une enquête judiciaire concomitante ne peuvent être transmises qu'avec l'accord de la juridiction ou du magistrat saisi du dossier.

Chapitre 4 – *La protection des infrastructures critiques*

Art. 4. La protection de l'infrastructure critique comprend l'ensemble des activités visant à prévenir, à atténuer ou à neutraliser le risque d'une réduction ou d'une discontinuité de la disponibilité de fournitures ou de services indispensables à la sauvegarde des intérêts vitaux ou des besoins essentiels de tout ou partie du pays ou de la population offerts par l'intermédiaire de l'infrastructure ainsi que le risque externe dont l'infrastructure est susceptible de faire l'objet.

Un point, système ou partie de celui-ci ne répondant pas à la définition donnée à l'article 2, peut être recensé et classifié comme infrastructure critique lorsque le fonctionnement d'une infrastructure critique en dépend.

De même peut être recensé et désigné comme infrastructure critique un secteur ou une partie de secteur dont tous les éléments ne répondent pas nécessairement à la définition donnée à l'article 2, mais dont l'ensemble est considéré comme tel.

Art. 5. Les modalités du recensement et de la désignation des infrastructures critiques sont fixées par règlement grand-ducal.

Art. 6. Le propriétaire ou opérateur d'une infrastructure critique est tenu de mettre à la disposition du Haut-Commissariat à la Protection nationale toutes les données sollicitées aux fins du recensement, de la désignation et de la protection des infrastructures critiques. Ces données comprennent toutes les informations qui sont nécessaires dans le contexte de la prévention ou de la gestion d'une crise.

Les données relatives à l'infrastructure critique faisant l'objet d'un enregistrement, d'une communication, d'une déclaration, d'un recensement, d'un classement, d'une autorisation ou d'une notification imposés par la loi ou par la réglementation afférente sont communiquées au Haut-Commissariat à la Protection nationale, sur sa demande, par les départements ministériels, les administrations et services de l'État qui détiennent ces données.

Art. 7. La désignation d'une infrastructure critique fait l'objet d'un arrêté grand-ducal.

Art. 8. (1) Le propriétaire ou opérateur d'une infrastructure critique est tenu d'élaborer un plan de sécurité et de continuité de l'activité qui comporte les mesures de sécurité pour la protection de l'infrastructure. Le Haut-Commissariat à la Protection nationale adresse au propriétaire ou à l'opérateur d'une infrastructure critique des recommandations concernant ces mesures de sécurité qui permettent d'en assurer la protection au sens de l'article ~~5~~4, d'en améliorer la résilience et de faciliter la gestion d'une crise.

(2) Le propriétaire ou opérateur d'une infrastructure critique est tenu de désigner un correspondant pour la sécurité qui exerce la fonction de contact pour les questions liées à la sécurité de l'infrastructure avec le Haut-Commissariat à la Protection nationale.

(3) Le propriétaire ou opérateur d'une infrastructure critique doit notifier au Haut-Commissariat à la Protection nationale tout incident ayant eu un impact significatif sur la sécurité et la pérennité du fonctionnement de l'infrastructure.

(4) La structure des plans de sécurité et de continuité de l'activité des infrastructures critiques est fixée par règlement grand-ducal.

Art. 9. En cas d'imminence ou de survenance d'une crise, le propriétaire ou opérateur d'une infrastructure critique, qui doit être, sauf en cas d'extrême urgence, dûment averti, est tenu de donner libre accès aux agents du Haut-Commissariat à la Protection nationale aux installations, locaux, terrains, aménagements faisant partie de l'infrastructure visée par la présente loi et les règlements à prendre en vue de son application.

Les actions de visite ou de contrôle entreprises sur place respectent le principe de proportionnalité.

Les dispositions reprises aux alinéas qui précèdent ne sont pas applicables aux locaux qui servent à l'habitation.

Chapitre 4bis – *La stratégie nationale en matière de sécurité des réseaux et des systèmes d'information*

Art. 9bis. Le Haut-Commissariat à la Protection nationale élabore une stratégie nationale en matière de sécurité des réseaux et des systèmes d'information, qui porte, en particulier, sur les points suivants :

h) les objectifs et les priorités de la stratégie nationale en matière de sécurité des réseaux et des systèmes d'information ;

i) un cadre de gouvernance permettant d'atteindre les objectifs et les priorités de la stratégie nationale en matière de sécurité des réseaux et des systèmes d'information, prévoyant notamment les rôles et les responsabilités des organismes publics et des autres acteurs pertinents ;

j) l'inventaire des mesures en matière de préparation, d'intervention et de récupération, y compris la coopération entre les secteurs public et privé ;

k) un aperçu des programmes d'éducation, de sensibilisation et de formation en rapport avec la stratégie nationale en matière de sécurité des réseaux et des systèmes d'information ;

l) un aperçu des plans de recherche et de développement en rapport avec la stratégie nationale en matière de sécurité des réseaux et des systèmes d'information ;

m) un plan d'évaluation des risques permettant d'identifier les risques ;

n) une liste des différents acteurs concernés par la mise en œuvre de la stratégie nationale en matière de sécurité des réseaux et des systèmes d'information.

Chapitre 5 – *Le personnel du Haut-Commissariat à la Protection nationale*

Art. 10. La nomination à la fonction de Haut-Commissaire à la Protection nationale se fait par arrêté grand-ducal sur proposition du membre du Gouvernement ayant dans ses attributions la Protection nationale.

Le Haut-Commissaire à la Protection nationale est responsable de la gestion de l'administration. Il en est le chef hiérarchique.

Art. 11. (1) Le cadre du personnel comprend un Haut-Commissaire à la Protection nationale et des fonctionnaires des différentes catégories de traitement telles que prévues par la loi modifiée du 25 mars 2015 fixant le régime des traitements et les conditions et modalités d'avancement des fonctionnaires de l'État.

(2) Le cadre du personnel peut être complété par des employés et salariés de l'État dans la limite des crédits budgétaires.

Le détachement des agents appelés au Haut-Commissariat à la Protection nationale se fait par arrêté du membre du Gouvernement ayant dans ses attributions la Protection nationale avec l'accord du ministre du ressort duquel relève l'agent en cause.

Art. 12. Un règlement grand-ducal détermine les modalités d'organisation des stages, des examens de fin de stage et des examens de promotion pour le personnel du Haut-Commissariat à la Protection nationale.

Chapitre 6 – *Dispositions spéciales*

Art. 13. En cas d'imminence ou de survenance d'une crise, le Conseil de Gouvernement assure la coordination des mesures de réquisition prévues par la loi du 8 décembre 1981 sur les réquisitions en cas de conflit armé, de crise internationale grave ou de catastrophe, par le titre V de la loi modifiée du 31 mai 1999 portant création d'un corps de police grand-ducale et d'une inspection générale de la police, ainsi que par le chapitre 4 de la loi communale modifiée du 13 décembre 1988.

Art. 14. Le Haut-Commissariat à la Protection nationale peut traiter les données personnelles nécessaires à l'exécution de la mission définie à l'article 3. Ces traitements sont soumis à la procédure d'autorisation préalable de la Commission nationale pour la protection des données telle que prévue à l'article 14 de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel.

Chapitre 7 – *Dispositions modificatives, transitoires et spéciales*

Art. 15. (1) Les fonctionnaires et employés visés à l'article 11 et relevant de la rubrique «Administration générale» telle qu'énoncée à l'article 12 de la loi modifiée du 25 mars 2015 fixant le régime des traitements et les conditions et modalités d'avancement des fonctionnaires de l'État, en service auprès du Haut-Commissariat à la Protection nationale au moment de l'entrée en vigueur de la présente loi, sont intégrés dans le cadre du personnel du Haut-Commissariat à la Protection nationale aux grade et échelon atteints au moment de l'entrée en vigueur de la présente loi.

(2) Les fonctionnaires détachés au Haut-Commissariat à la Protection nationale au moment de la mise en vigueur de la présente loi, intégrés dans le cadre du personnel du Haut-Commissariat à la

Protection nationale, et qui d'après la législation en vigueur dans leur service d'origine au moment de leur détachement avaient une perspective de carrière plus favorable pour l'accès aux différentes fonctions de leur carrière, conservent leurs anciennes possibilités d'avancement.

Art. 16. À l'article 16 de la loi du 23 juillet 1952 concernant l'organisation militaire, telle qu'elle a été modifiée dans la suite, il est inséré un nouveau point libellé comme suit: «2) les officiers, les sous-officiers et les caporaux de carrière employés par ordre du Gouvernement auprès du Haut-Commissariat à la Protection nationale.»

L'actuel point 2) devient le point 3).

Art. 17. La loi modifiée du 25 mars 2015 fixant le régime des traitements et les conditions et modalités d'avancement des fonctionnaires de l'État est modifiée comme suit:

(1) à l'article 12, paragraphe 1er, alinéa 7, point 11°, les termes «de Haut-Commissaire à la Protection nationale,» sont insérés avant les termes «et de directeur de différentes administrations»;

(2) dans l'annexe A «Classification des fonctions», Catégorie de traitement A, Groupe de traitement A1, Sous-groupe à attributions particulières, il est ajouté la mention «Haut-Commissaire à la Protection nationale» au grade 17;

(3) au paragraphe b) de l'article 17, il est inséré, à la suite des termes «inspecteur général de la sécurité dans la Fonction publique», la mention «Haut-Commissaire à la Protection nationale».

Art. 18. La loi du 8 décembre 1981 sur les réquisitions en cas de conflit armé, de crise internationale grave ou de catastrophe, est modifiée comme suit:

1) au chapitre Ier, article 1er, dernière phrase, il est ajouté en fin de phrase: «ou d'une crise, au sens de la loi portant création d'un Haut-Commissariat à la Protection nationale et modifiant a) la loi modifiée du 23 juillet 1952 concernant l'organisation militaire, b) la loi du 8 décembre 1981 sur les réquisitions en cas de conflit armé, de crise internationale grave ou de catastrophe, c) la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel, d) la loi modifiée du 25 juin 2009 sur les marchés publics, e) la loi modifiée du 9 décembre 2005 déterminant les conditions et modalités de nomination de certains fonctionnaires occupant des fonctions dirigeantes dans les administrations et services de l'État, f) la loi modifiée du 25 mars 2015 fixant le régime des traitements et les conditions et modalités d'avancement des fonctionnaires de l'État».

2) au chapitre IV, article 8 b) *in fine*, il est ajouté: «5) Les agents du Haut-Commissariat à la Protection nationale».

Art. 19. Au chapitre III, article 14 (1) de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel, il est ajouté *in fine* un point (h):

«(h) les traitements concernant la prévention et la gestion de crises conformément à l'article 14 de la loi du 23 juillet 2016 portant création d'un Haut-Commissariat à la Protection nationale et modifiant a) la loi modifiée du 23 juillet 1952 concernant l'organisation militaire, b) la loi du 8 décembre 1981 sur les réquisitions en cas de conflit armé, de crise internationale grave ou de catastrophe, c) la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel, d) la loi modifiée du 25 juin 2009 sur les marchés publics, e) la loi modifiée du 9 décembre 2005 déterminant les conditions et modalités de nomination de certains fonctionnaires occupant des fonctions dirigeantes dans les administrations et services de l'État, f) la loi modifiée du 25 mars 2015 fixant le régime des traitements et les conditions et modalités d'avancement des fonctionnaires de l'État».

Art. 20. À l'article 1er de la loi modifiée du 9 décembre 2005 déterminant les conditions et modalités de nomination de certains fonctionnaires occupant des fonctions dirigeantes dans les administrations et services de l'État, telle qu'elle a été modifiée dans la suite, il est inséré un tiret supplémentaire libellé comme suit: «– de Haut-Commissaire à la Protection nationale.»

Art. 21. Au livre Ier, titre III, chapitre III, article 8 (1) de la loi modifiée du 25 juin 2009 sur les marchés publics, il est ajouté *in fine* un point l):

«l) pour les marchés de la protection nationale:

a) pour les fournitures ou services qui sont déclarés secrets;

b) pour les fournitures ou services nécessaires à la protection des intérêts vitaux ou des besoins essentiels de tout ou partie du pays ou de la population, et en particulier les fournitures ou services relatifs à la prévention et la gestion de crises;

c) pour les fournitures d'effets d'équipement et de matériel d'intervention ainsi que d'effets personnels de protection et de sécurité des membres des unités d'intervention.»

Art. 22. La référence à la présente loi pourra se faire sous une forme abrégée en utilisant les termes «loi du 23 juillet 2016 portant création d'un Haut-Commissariat à la Protection nationale».

Art. 23. La présente loi entre en vigueur le premier jour du deuxième mois qui suit sa publication au Mémorial.

Mandons et ordonnons que la présente loi soit insérée au Mémorial pour être exécutée et observée par tous ceux que la chose concerne.

*

RESUME DU PROJET DE LOI

Le projet de loi transpose en droit luxembourgeois 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 (*directive on security of network and information systems*, ci-après directive « NIS »). La directive a pour objet de renforcer, sur base de règles harmonisées, la cybersécurité au niveau des Etats membres et de consolider la coopération transfrontalière en matière de gestion des risques cyber.

i) Le projet de loi fixe d'abord des obligations minimales en matière de sécurité des réseaux et des systèmes d'information à respecter par les « opérateurs de services essentiels » (OSE), c'est-à-dire des entreprises qui offrent un service important pour la société et l'économie et qui agissent dans un des secteurs suivants : l'énergie (électricité, pétrole et gaz), les transports (aérien, ferroviaire, par voie d'eau et routier), les services bancaires (établissements de crédit), les infrastructures de marchés financiers (plateformes de négociation, contreparties centrales), la santé (prestataires de soins de santé), l'eau (fourniture et distribution d'eau potable) ou encore les infrastructures numériques. Ces opérateurs auront désormais l'obligation d'assurer un niveau de sécurité adéquat de leurs réseaux et systèmes d'information et de notifier à l'autorité nationale compétente les incidents qui ont un impact significatif sur la continuité de leurs services essentiels.

ii) Des exigences similaires sont prévues pour garantir la sécurité des réseaux et des systèmes d'information des « fournisseurs de services numériques » (FSN), c'est-à-dire les places de marché en ligne, les moteurs de recherche en ligne et les services informatiques en nuage.

iii) Répondant aux obligations inscrites dans la directive, le projet de loi désigne les autorités nationales compétentes, crée un point de contact unique en matière de coopération transfrontalière et donne une base légale à l'élaboration d'une stratégie nationale en matière de sécurité des réseaux et des systèmes d'information.

   a. L'Institut luxembourgeois de régulation (ILR) et la Commission de surveillance du secteur financier (CSSF) seront les autorités nationales compétentes chargées de veiller au respect par les opérateurs de services essentiels et les fournisseurs de services numériques des obligations en matière de sécurité des réseaux et des systèmes d'information. Etant donné que la « directive NIS » s'applique aux entreprises actives dans sept secteurs et que l'ILR régule d'ores et déjà une grande partie de ces secteurs avec des règles similaires à celles prévues dans la « directive NIS », tout en disposant d'une expertise confirmée en matière de régulation, ainsi que d'un statut d'indépendance, il est proposé de lui confier la mission d'autorité compétente dans le sens de la directive NIS, à l'exception des secteurs des banques et des infrastructures de marchés financiers, pour lesquels la CSSF est l'autorité régulatrice.

      Dans le cadre de leur nouvelle mission de réception des notifications des incidents de sécurité de la part des opérateurs de services essentiels et des fournisseurs de services numériques, l'ILR et la CSSF collaboreront avec le Centre de traitement des urgences informatiques (CERT Gouvernemental) et le Computer Incident Response Center Luxembourg (CIRCL) qui disposent

d'une expertise avérée en matière de traitement des incidents informatiques. Tandis que le CERT Gouvernemental est l'entité gestionnaire d'incidents du réseau étatique, le CIRCL assure ce rôle au niveau du secteur privé.

Un contrat de collaboration formalisera la coopération entre les deux autorités compétentes et les deux entités gestionnaires d'incidents informatiques.

b) L'ILR assurera le rôle de point de contact national unique dans le cadre de la « directive NIS ». Ainsi, il reviendra à l'ILR d'assurer la coopération transfrontalière en la matière.

c) Enfin, la « directive NIS » impose aux Etats membres d'élaborer une stratégie nationale en matière de sécurité des réseaux et des systèmes d'information définissant les objectifs stratégiques et les actions politiques concrètes à mettre en œuvre. Cette mission sera inscrite dans la loi organique du Haut-Commissariat à la Protection nationale (HCPN). Etant donné que cette stratégie nationale en matière de sécurité des réseaux et des systèmes d'information peut être considérée comme équivalente à une stratégie nationale de cybersécurité et que le Luxembourg dispose déjà d'une telle stratégie nationale en matière de cybersécurité, élaborée par un comité interministériel présidé par le HCPN, la nouvelle loi fortifie ce rôle de coordinateur en lui accordant une assise juridique dans la loi HCPN.

iv) En ce qui concerne le cadre institutionnel en matière de cybersécurité, il a été jugé indiqué, sur base de l'expérience des dernières années, d'assurer une séparation nette entre l'autorité qui élabore les politiques de sécurité (ANSSI) et l'autorité qui veille à ce que les produits cryptographiques soient conformes à ces politiques de sécurité. Ainsi, le projet de loi transfère la mission d'autorité d'agrément cryptographique de l'ANSSI au Centre des technologies de l'information de l'Etat (CTIE).

*

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 PARLEMENT EUROPÉEN ET LE CONSEIL DE L'UNION EUROPÉENNE,

vu le traité sur le fonctionnement de l'Union européenne, et notamment son article 114,

vu la proposition de la Commission européenne,

après transmission du projet d'acte législatif aux parlements nationaux,

vu l'avis du Comité économique et social européen ([1]),

statuant conformément à la procédure législative ordinaire ([2]),

considérant ce qui suit:

(1) Les réseaux et les services et systèmes d'information jouent un rôle crucial dans la société. Leur fiabilité et leur sécurité sont essentielles aux fonctions économiques et sociétales et notamment au fonctionnement du marché intérieur.

(2) L'ampleur, la fréquence et l'impact des incidents de sécurité ne cessent de croître et représentent une menace considérable pour le fonctionnement des réseaux et des systèmes d'information. Ces systèmes peuvent également devenir des cibles pour des actions intentionnelles malveillantes qui visent à la détérioration ou à l'interruption de leur fonctionnement. Ces incidents peuvent nuire à l'exercice d'activités économiques, entraîner des pertes financières importantes, entamer la confiance des utilisateurs et porter un grand préjudice à l'économie de l'Union.

(3) Les réseaux et les systèmes d'information, principalement l'internet, revêtent une importance essentielle pour la circulation transfrontalière des biens, des services et des personnes. En raison de ce caractère transnational, toute perturbation importante de ces systèmes, qu'elle soit intentionnelle ou non et indépendamment du lieu où elle se produit, peut avoir une incidence sur certains États membres et sur l'Union dans son ensemble. La sécurité des réseaux et des systèmes d'information est donc essentielle au fonctionnement harmonieux du marché intérieur.

(4) En se fondant sur les progrès significatifs accomplis au sein du Forum européen des États membres pour favoriser les discussions et les échanges de bonnes pratiques, et notamment l'élaboration de principes relatifs à la coopération européenne en cas de crise dans le domaine de la cybersécurité, il convient de constituer un groupe de coopération réunissant des représentants des États membres, de la Commission et de l'Agence de l'Union européenne chargée de la sécurité des réseaux et de l'information (ENISA) ayant pour mission de soutenir et de faciliter la coopération stratégique entre les États membres en ce qui concerne la sécurité des réseaux et des

([1]) JO C 271 du 19.9.2013, p. 133.
([2]) Position du Parlement européen du 13 mars 2014 (non encore parue au Journal officiel) et position du Conseil en première lecture du 17 mai 2016 (non encore parue au Journal officiel). Position du Parlement européen du 6 juillet 2016 (non encore parue au Journal officiel).

systèmes d'information. Pour que ce groupe soit efficace et ouvert à tous, il est essentiel que tous les États membres soient dotés d'un minimum de moyens et d'une stratégie garantissant un niveau élevé de sécurité des réseaux et des systèmes d'information sur leur territoire. De plus, les opérateurs de services essentiels et les fournisseurs de service numérique devraient être soumis à des exigences en matière de sécurité et de notification, afin de promouvoir une culture de gestion des risques et de faire en sorte que les incidents les plus graves soient signalés.

(5) Les moyens existants ne sont pas suffisants pour assurer un niveau élevé de sécurité des réseaux et des systèmes d'information dans l'Union. Les niveaux de préparation sont très différents selon les États membres, ce qui se traduit par une fragmentation des approches dans l'Union. Les niveaux de protection des consommateurs et des entreprises sont donc inégaux, ce qui porte atteinte au niveau global de sécurité des réseaux et des systèmes d'information dans l'Union. En outre, l'absence d'exigences communes applicables aux opérateurs de services essentiels et aux fournisseurs de service numérique rend impossible la création d'un mécanisme général et efficace de coopération au niveau de l'Union. Les universités et les centres de recherche ont un rôle déterminant à jouer dans la stimulation de la recherche, du développement et de l'innovation dans ces domaines.

(6) Il faut donc, pour faire face efficacement aux défis que pose la sécurité des réseaux et des systèmes d'information, adopter une approche globale au niveau de l'Union qui couvrira des exigences minimales communes en matière de renforcement des capacités et de planification, l'échange d'informations, la coopération et des exigences communes en matière de sécurité pour les opérateurs de services essentiels et les fournisseurs de service numérique. Cependant, il n'est pas interdit aux opérateurs de services essentiels et aux fournisseurs de service numérique de mettre en œuvre des mesures de sécurité plus strictes que celles prévues par la présente directive.

(7) Pour que tous les incidents et risques pertinents soient couverts, il convient que la présente directive s'applique tant aux opérateurs de services essentiels qu'aux fournisseurs de service numérique. Cependant, les obligations imposées aux opérateurs de services essentiels et aux fournisseurs de service numérique ne devraient pas s'appliquer aux entreprises qui fournissent des réseaux de communications publics ou des services de communications électroniques accessibles au public au sens de la directive 2002/21/CE du Parlement européen et du Conseil ([1]), qui sont soumises aux exigences particulières relatives à la sécurité et à l'intégrité énoncées dans ladite directive, ni aux prestataires de services de confiance au sens du règlement (UE) nº 910/2014 du Parlement européen et du Conseil ([2]), qui sont soumis aux exigences de sécurité énoncées dans ledit règlement.

(8) La présente directive devrait s'entendre sans préjudice de la possibilité donnée à chaque État membre d'adopter les mesures nécessaires pour garantir la protection des intérêts essentiels de sa sécurité, assurer l'action publique et la sécurité publique et permettre la recherche, la détection et la poursuite d'infractions pénales. Conformément à l'article 346 du traité sur le fonctionnement de l'Union européenne, aucun État membre n'est tenu de fournir des renseignements dont il estimerait la divulgation contraire aux intérêts essentiels de sa sécurité. À cet égard, la décision 2013/488/UE du Conseil ([3]) et les accords de non-divulgation, ou les accords de non-divulgation informelle tels que le protocole d'échange d'information «Traffic Light Protocol», sont pertinents.

(9) Certains secteurs de l'économie sont déjà réglementés ou peuvent l'être à l'avenir par des actes juridiques sectoriels de l'Union comportant des règles relatives à la sécurité des réseaux et des systèmes d'information. Chaque fois que ces actes juridiques de l'Union contiennent des dispositions imposant des exigences relatives à la sécurité des réseaux et des systèmes d'information ou à la notification des incidents, ces dispositions devraient s'appliquer si elles contiennent des exigences ayant un effet au moins équivalent à celui des obligations figurant dans la présente directive. Les États membres devraient alors appliquer les dispositions des actes juridiques sectoriels concernés de l'Union, notamment celles relatives à la compétence, et ils ne devraient pas mettre en œuvre le processus d'identification des opérateurs de services essentiels tel qu'il est défini par la présente directive. À cet égard, les États membres devraient fournir à la Commission des informations sur l'application de telles dispositions de *lex specialis*. Pour établir si les exigences relatives à la sécurité des réseaux et des systèmes d'information et à la notification des incidents prévues par les actes juridiques sectoriels de l'Union sont équivalentes à celles qui sont énoncées dans la présente directive, il ne devrait être tenu compte que des dispositions des actes juridiques pertinents de l'Union et de leur application dans les États membres.

(10) Dans le secteur des transports par voie d'eau, les exigences en matière de sécurité imposées par des actes juridiques de l'Union aux compagnies, aux navires, aux installations portuaires, aux ports et aux services de gestion du trafic maritime portent sur l'ensemble des activités, y compris les systèmes de radio et de télécommunications, les systèmes informatiques et les réseaux. Une partie des procédures auxquelles il est obligatoire de se conformer concerne le signalement de tous les incidents et devrait donc être considérée comme une *lex specialis*, dans la mesure où ces exigences sont au moins équivalentes aux dispositions correspondantes de la présente directive.

([1]) Directive 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 (directive «cadre») (JO L 108 du 24.4.2002, p. 33).

([2]) Règlement (UE) nº 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 (JO L 257 du 28.8.2014, p. 73).

([3]) Décision 2013/488/UE du Conseil du 23 septembre 2013 concernant les règles de sécurité aux fins de la protection des informations classifiées de l'Union européenne (JO L 274 du 15.10.2013, p. 1).

(11) Lors de l'identification des opérateurs dans le secteur des transports par voie d'eau, les États membres devraient prendre en compte les codes internationaux et les lignes directrices existants et futurs élaborés notamment par l'Organisation maritime internationale, en vue d'offrir une approche cohérente aux différents opérateurs maritimes.

(12) La réglementation et la surveillance dans les secteurs de la banque et des infrastructures des marchés financiers sont hautement harmonisées au niveau de l'Union au moyen de dispositions du droit primaire et du droit dérivé de l'Union et de normes élaborées en collaboration avec les autorités européennes de surveillance. Au sein de l'union bancaire, l'application et la surveillance de ces exigences sont assurées par le mécanisme de surveillance unique. Pour les États membres qui ne font pas partie de l'union bancaire, ces fonctions sont assurées par leurs organes nationaux de réglementation bancaire compétents. Dans d'autres domaines de la réglementation du secteur financier, le système européen de surveillance financière garantit également un degré élevé d'uniformité et de convergence des pratiques en matière de surveillance. L'Autorité européenne des marchés financiers joue également un rôle direct de surveillance pour certaines entités, à savoir les agences de notation de crédit et les référentiels centraux.

(13) Le risque opérationnel est un élément crucial de la réglementation et de la surveillance prudentielles dans les secteurs de la banque et des infrastructures de marchés financiers. Il porte sur toutes les activités, notamment la sécurité, l'intégrité et la résilience des réseaux et des systèmes d'information. Les exigences concernant ces systèmes, qui vont souvent au-delà des exigences prévues en vertu de la présente directive, sont définies dans un certain nombre d'actes juridiques de l'Union, y compris les règles concernant l'accès à l'activité des établissements de crédit et la surveillance prudentielle des établissements de crédit et des entreprises d'investissement, ainsi que les règles concernant les exigences prudentielles applicables aux établissements de crédit et aux entreprises d'investissement, parmi lesquelles figurent les exigences concernant le risque opérationnel; les règles concernant les marchés d'instruments financiers, qui comprennent des exigences relatives à l'évaluation des risques pour les entreprises d'investissement et les marchés réglementés; les règles relatives aux instruments dérivés de gré à gré, aux contreparties centrales et aux référentiels centraux, parmi lesquelles figurent les exigences concernant le risque opérationnel applicables aux contreparties centrales et aux référentiels centraux; et les règles concernant l'amélioration du règlement de titres dans l'Union et les dépositaires centraux de titres, parmi lesquelles figurent les exigences concernant le risque opérationnel. En outre, les obligations en matière de notification des incidents font partie des pratiques de surveillance normales dans le secteur financier et sont souvent incluses dans les manuels de surveillance. Les États membres devraient tenir compte de ces règles et exigences au moment d'appliquer la *lex specialis*.

(14) Comme le fait observer la Banque centrale européenne dans son avis du 25 juillet 2014 ([1]), la présente directive n'a pas d'incidence sur le régime mis en place dans le droit de l'Union pour la surveillance des systèmes de paiement et de règlement dans le cadre de l'Eurosystème. Il serait opportun que les autorités chargées de cette surveillance procèdent à des échanges d'expériences sur les questions relatives à la sécurité des réseaux et des systèmes d'information avec les autorités compétentes en vertu de la présente directive. La même considération s'applique aux membres du Système européen de banques centrales qui n'appartiennent pas à la zone euro et qui exercent cette surveillance des systèmes de paiement et de règlement sur la base de leurs dispositions législatives et réglementaires nationales.

(15) Une place de marché en ligne permet aux consommateurs et aux professionnels de conclure des contrats de vente ou de service en ligne avec des professionnels et c'est la destination finale pour la conclusion desdits contrats. Elle ne devrait pas concerner les services en ligne qui ne servent que d'intermédiaires pour des services fournis par un tiers à travers lequel un contrat peut en définitive être conclu. Elle ne devrait donc pas concerner les services en ligne qui comparent le prix de certains produits ou services de plusieurs professionnels, avant de réorienter l'utilisateur vers le professionnel choisi en vue de l'achat du produit. Parmi les services informatiques fournis par la place de marché en ligne peuvent figurer le traitement de transactions, l'agrégation de données ou le profilage d'utilisateurs. Les magasins d'applications en ligne, qui fonctionnent comme des magasins en ligne permettant la distribution numérique d'applications ou de logiciels émanant de tiers, doivent s'entendre comme étant un type de place de marché en ligne.

(16) Un moteur de recherche en ligne permet à l'utilisateur d'effectuer des recherches sur, en principe, tous les sites internet sur la base d'une requête lancée sur n'importe quel sujet. Il peut aussi se limiter aux sites internet dans une langue donnée. La définition d'un moteur de recherche en ligne donnée par la présente directive ne devrait pas s'appliquer aux fonctions de recherche qui se limitent au contenu d'un site internet spécifique, indépendamment de la question de savoir si la fonction de recherche est assurée par un moteur de recherche externe. Elle ne devrait pas non plus concerner les services en ligne qui comparent le prix de certains produits ou services de différents professionnels et qui réorientent ensuite l'utilisateur vers le professionnel choisi en vue de l'achat du produit.

(17) Les services d'informatique en nuage couvrent un vaste éventail d'activités qui peuvent être fournies selon différents modèles. Aux fins de la présente directive, les termes «services d'informatique en nuage» couvrent des services qui permettent l'accès à un ensemble modulable et variable de ressources informatiques pouvant être partagées. Ces ressources informatiques comprennent des ressources telles que les réseaux, serveurs et autres

([1]) JO C 352 du 7.10.2014, p. 4.

infrastructures, le stockage, les applications et les services. Le terme «modulable» renvoie aux ressources informatiques qui sont attribuées d'une manière souple par le fournisseur de services en nuage, indépendamment de la localisation géographique de ces ressources, pour gérer les fluctuations de la demande. Les termes «ensemble variable» sont utilisés pour décrire les ressources informatiques qui sont mobilisées et libérées en fonction de la demande pour pouvoir augmenter ou réduire rapidement les ressources disponibles en fonction de la charge de travail. Les termes «pouvant être partagées» sont utilisés pour décrire les ressources informatiques qui sont mises à disposition de nombreux utilisateurs qui partagent un accès commun au service, le traitement étant effectué séparément pour chaque utilisateur bien que le service soit fourni à partir du même équipement électronique.

(18) La fonction d'un point d'échange internet (IXP) est d'interconnecter des réseaux. Un IXP ne fournit pas d'accès à un réseau et n'agit pas en tant que fournisseur ou opérateur de transit. Un IXP ne fournit pas non plus d'autres services non liés à l'interconnexion, sans que cela empêche l'exploitant d'un IXP de fournir des services non liés. Un IXP a pour fonction d'interconnecter des réseaux qui sont distincts d'un point de vue technique et organisationnel. Les termes «système autonome» sont utilisés pour désigner un réseau autonome sur le plan technique.

(19) Les États membres devraient être chargés d'établir quelles sont les entités qui remplissent les critères de la définition d'un opérateur de services essentiels. Dans le souci d'assurer une démarche cohérente, la définition d'un opérateur de services essentiels devrait être appliquée de manière cohérente par tous les États membres. À cette fin, la présente directive prévoit l'évaluation des entités actives dans les secteurs et sous-secteurs spécifiques, l'établissement d'une liste de services essentiels, la prise en considération d'une liste commune des facteurs transsectoriels pour déterminer si un incident potentiel aurait un effet disruptif important, un processus de consultation faisant intervenir les États membres concernés dans le cas d'entités fournissant des services dans plus d'un État membre, et le soutien apporté par le groupe de coopération dans le cadre du processus d'identification. Afin qu'il soit fidèlement tenu compte des éventuels changements intervenus sur le marché, il convient que la liste des opérateurs identifiés soit régulièrement revue par les États membres et mise à jour si nécessaire. Enfin, les États membres devraient communiquer à la Commission les informations nécessaires à l'appréciation de la mesure dans laquelle cette méthode commune a permis de procéder à une application cohérente de la définition par les États membres.

(20) Dans le cadre du processus d'identification des opérateurs de services essentiels, il convient que les États membres évaluent, au moins pour chaque sous-secteur visé par la présente directive, quels services doivent être considérés comme essentiels au maintien de fonctions sociétales et économiques critiques et jugent si les entités qui sont énumérées pour les secteurs et sous-secteurs visés dans la présente directive et qui fournissent ces services remplissent les critères requis pour l'identification des opérateurs. Pour apprécier si une entité fournit un service qui est essentiel au maintien de fonctions sociétales ou économiques critiques, il suffit d'examiner si cette entité fournit un service figurant dans la liste des services essentiels. En outre, il y a lieu de démontrer que la fourniture du service essentiel dépend des réseaux et des systèmes d'information. Enfin, lorsqu'ils évaluent si un incident aurait un effet disruptif important sur la fourniture du service, les États membres devraient tenir compte d'un certain nombre de facteurs transsectoriels ainsi que, le cas échéant, de facteurs sectoriels.

(21) Aux fins d'identification des opérateurs de services essentiels, l'établissement dans un État membre suppose l'exercice effectif et réel d'une activité au moyen d'une installation stable. La forme juridique retenue pour un tel établissement, qu'il s'agisse d'une succursale ou d'une filiale ayant la personnalité juridique, n'est pas déterminante à cet égard.

(22) Il est possible que les entités relevant des secteurs et sous-secteurs visés dans la présente directive fournissent des services essentiels et des services non essentiels. Par exemple, dans le secteur du transport aérien, les aéroports fournissent des services qu'un État membre pourrait considérer comme essentiels, tels que la gestion des pistes, mais aussi un certain nombre de services qui pourraient être considérés comme non essentiels, tels que la mise à disposition de zones commerciales. Les opérateurs de services essentiels ne devraient être soumis aux exigences de sécurité spécifiques que pour les services qui sont jugés essentiels. Aux fins de l'identification des opérateurs, les États membres devraient dès lors établir une liste des services qui sont considérés comme essentiels.

(23) La liste des services devrait contenir tous les services fournis sur le territoire d'un État membre donné qui satisfont aux exigences prévues par la présente directive. Les États membres devraient être en mesure de compléter la liste existante en y incluant de nouveaux services. La liste des services devrait servir de point de référence aux États membres, en permettant d'identifier les opérateurs de services essentiels. Son objectif est d'identifier les types de services essentiels dans un secteur donné visé dans la présente directive, en les distinguant ainsi des activités non essentielles dont une entité active dans un secteur donné pourrait avoir la responsabilité. La liste des services établie par chaque État membre constituerait une contribution supplémentaire à l'évaluation des pratiques réglementaires de chaque État membre dans le but d'assurer la cohérence générale du processus d'identification dans les États membres.

(24) Aux fins du processus d'identification, lorsqu'une entité fournit un service essentiel dans deux ou plusieurs États membres, les États membres en question devraient entamer des consultations bilatérales ou multilatérales entre eux. Ce processus de consultation est destiné à les aider à évaluer le caractère critique de l'opérateur en termes d'incidence transfrontalière en permettant ainsi à chaque État membre concerné de présenter son point de vue sur les risques associés aux services fournis. Lors de ce processus, les États membres concernés devraient tenir compte de leurs avis respectifs et ils devraient pouvoir solliciter l'assistance du groupe de coopération à cet égard.

(25) À la suite du processus d'identification, les États membres devraient adopter des mesures nationales visant à établir quelles entités sont soumises à des obligations en matière de sécurité des réseaux et des systèmes d'information. Ce résultat pourrait être atteint par l'adoption d'une liste énumérant tous les opérateurs de services essentiels ou par l'adoption de mesures nationales assorties de critères objectifs quantifiables, tels que la production de l'opérateur ou le nombre d'utilisateurs, qui permettent de déterminer quelles sont les entités qui sont soumises à des obligations en matière de sécurité des réseaux et des systèmes d'information. Les mesures nationales, que ces mesures soient préexistantes ou qu'elles soient adoptées dans le cadre de la présente directive, devraient inclure toutes les mesures juridiques, administratives et politiques permettant d'identifier des opérateurs de services essentiels conformément à la présente directive.

(26) Afin de montrer l'importance, par rapport au secteur concerné, des opérateurs identifiés de services essentiels, les États membres devraient tenir compte du nombre et de la taille de ces opérateurs, par exemple en termes de parts de marché ou de quantité produite ou transportée, sans être contraints de divulguer des informations susceptibles de révéler l'identité des opérateurs identifiés.

(27) Afin de déterminer si un incident est susceptible d'avoir un effet disruptif important sur la fourniture d'un service essentiel, les États membres devraient prendre en compte plusieurs facteurs différents, tels que le nombre d'utilisateurs s'appuyant sur ce service à des fins privées ou professionnelles. Ce service peut s'utiliser de manière directe, indirecte ou à travers un intermédiaire. Lorsqu'ils évaluent l'impact qu'un incident pourrait avoir, du point de vue de son intensité et de sa durée, sur les fonctions économiques et sociétales ou sur la sûreté publique, les États membres devraient également estimer le temps qui pourrait s'écouler avant que l'interruption du service ne commence à avoir un impact négatif.

(28) Afin de déterminer si un incident est susceptible d'avoir un effet disruptif important sur la fourniture d'un service essentiel, il convient, outre les facteurs transsectoriels, de prendre également en compte des facteurs sectoriels. Ces facteurs pourraient inclure, pour les fournisseurs d'énergie, le volume ou la proportion d'énergie produite au niveau national; pour les fournisseurs de pétrole, le volume journalier; pour le transport aérien, y compris les aéroports et les transporteurs aériens, le transport ferroviaire et les ports maritimes, la proportion du volume de trafic national et le nombre de passagers ou d'opérations de fret par an; pour les infrastructures bancaires ou des marchés financiers, leur importance systémique sur la base de leurs actifs totaux ou du ratio entre ces actifs totaux et le PIB; pour le secteur de la santé, le nombre annuel de patients pris en charge par le prestataire; pour la production, le traitement et la distribution d'eau, le volume d'eau, le nombre et les types d'utilisateurs servis, y compris, par exemple, des hôpitaux, des organismes de service public ou des particuliers, ainsi que l'existence d'autres sources d'approvisionnement en eau couvrant la même zone géographique.

(29) Pour atteindre un niveau élevé de sécurité des réseaux et des systèmes d'information et le maintenir, chaque État membre devrait se doter d'une stratégie nationale en matière de sécurité des réseaux et des systèmes d'information définissant les objectifs stratégiques et les actions politiques concrètes à mettre en œuvre.

(30) Compte tenu des divergences entre les structures de gouvernance nationales et en vue de sauvegarder les accords existants au niveau sectoriel ou les autorités de surveillance et de régulation de l'Union et d'éviter les doubles emplois, les États membres devraient pouvoir désigner plusieurs autorités nationales compétentes chargées d'accomplir les tâches liées à la sécurité des réseaux et des systèmes d'information des opérateurs de services essentiels et des fournisseurs de service numérique dans le cadre de la présente directive.

(31) Afin de faciliter la coopération et la communication transfrontalières et pour permettre la mise en œuvre effective de la présente directive, il est nécessaire que chaque État membre, sans préjudice des accords sectoriels de régulation, désigne un point de contact national unique chargé de coordonner les tâches liées à la sécurité des réseaux et des systèmes d'information et de la coopération transfrontalière au niveau de l'Union. Les autorités compétentes et les points de contact uniques devraient être dotés de ressources techniques, financières et humaines suffisantes pour pouvoir s'acquitter de manière effective et efficace des tâches qui leur sont dévolues et atteindre ainsi les objectifs de la présente directive. Étant donné que la présente directive vise à améliorer le fonctionnement du marché intérieur par l'instauration de la confiance, les organismes des États membres doivent être en mesure de coopérer efficacement avec les acteurs économiques et être structurés en conséquence.

(32) Les autorités compétentes ou les centres de réponse aux incidents de sécurité informatique (CSIRT) devraient recevoir les notifications d'incidents. Les points de contact uniques ne devraient pas recevoir directement toutes les notifications d'incidents, à moins qu'ils n'agissent également en qualité d'autorité compétente ou de CSIRT. Une autorité compétente ou un CSIRT devrait cependant pouvoir charger le point de contact unique de transmettre les notifications d'incidents aux points de contact uniques d'autres États membres touchés.

(33) Pour assurer l'information effective des États membres et de la Commission, un rapport de synthèse devrait être soumis par le point de contact unique au groupe de coopération et devrait être rendu anonyme afin de préserver la confidentialité des notifications et l'identité des opérateurs de services essentiels et des fournisseurs de service numérique, étant donné que les données relatives à l'identité des entités qui sont à l'origine de la notification ne sont pas requises pour l'échange de bonnes pratiques au sein du groupe de coopération. Le rapport de synthèse devrait contenir des informations sur le nombre de notifications reçues ainsi qu'une indication de la nature des incidents notifiés, telle que les types d'atteintes à la sécurité, leur gravité ou leur durée.

(34) Les États membres devraient disposer de moyens suffisants, sur les plans technique et organisationnel, pour prévenir et détecter les incidents et risques liés aux réseaux et systèmes d'information et prendre les mesures d'intervention et d'atténuation nécessaires. Les États membres devraient dès lors veiller à disposer de CSIRT, également connus sous la dénomination de centres de réponse aux urgences informatiques (CERT), opérationnels et conformes aux exigences essentielles afin de garantir l'existence de moyens effectifs et compatibles pour gérer les incidents et les risques et d'assurer une coopération efficace au niveau de l'Union. Afin que tous les types d'opérateurs de services essentiels et de fournisseurs de service numérique puissent bénéficier de ces moyens et de cette coopération, les États membres devraient veiller à ce que tous les types soient couverts par un CSIRT désigné. Compte tenu de l'importance de la coopération internationale en matière de cybersécurité, les CSIRT devraient pouvoir participer à des réseaux de coopération internationaux en plus du réseau des CSIRT institué par la présente directive.

(35) Étant donné que la plupart des réseaux et des systèmes d'information sont exploités par des intérêts privés, il est essentiel d'établir une coopération entre secteur public et secteur privé. Il convient d'encourager les opérateurs de services essentiels et les fournisseurs de service numérique à mettre en place leurs propres mécanismes informels de coopération pour garantir la sécurité des réseaux et des systèmes d'information. Le groupe de coopération devrait pouvoir inviter les parties prenantes concernées aux discussions, s'il y a lieu. Il est essentiel, pour encourager effectivement le partage des informations et des bonnes pratiques, de veiller à ce que les opérateurs de services essentiels et les fournisseurs de service numérique qui participent à ces échanges ne soient pas désavantagés du fait même de leur coopération.

(36) L'ENISA devrait assister les États membres et la Commission en mettant à leur disposition ses connaissances et ses conseils et en facilitant l'échange des bonnes pratiques. En particulier, la Commission devrait consulter l'ENISA et les États membres devraient pouvoir la consulter en ce qui concerne l'application de la présente directive. Afin de développer les moyens disponibles et la connaissance dans les États membres, le groupe de coopération devrait aussi être un outil d'échange des bonnes pratiques et d'examen des capacités et de l'état de préparation des États membres et, à titre volontaire, il devrait aider ses membres à évaluer leurs stratégies nationales en matière de sécurité des réseaux et des systèmes d'information, à renforcer leurs capacités et à évaluer les exercices relatifs à la sécurité des réseaux et des systèmes d'information.

(37) Le cas échéant, les États membres devraient pouvoir utiliser ou adapter les structures organisationnelles ou les stratégies existantes aux fins de l'application de la présente directive.

(38) Les tâches respectives du groupe de coopération et de l'ENISA sont interdépendantes et complémentaires. D'une manière générale, l'ENISA devrait aider le groupe de coopération dans l'accomplissement de ses tâches, conformément à l'objectif de l'ENISA défini au règlement (UE) nº 526/2013 du Parlement européen et du Conseil ([1]), qui consiste à assister les institutions, organes et organismes de l'Union et les États membres dans la mise en œuvre des politiques nécessaires pour satisfaire aux exigences légales et réglementaires requises au titre des actes juridiques existants et à venir de l'Union en matière de sécurité des réseaux et des systèmes d'information. En particulier, l'ENISA devrait fournir une assistance dans les domaines qui correspondent à ses propres missions telles que définies dans le règlement (UE) nº 526/2013, à savoir l'analyse des stratégies en matière de sécurité des réseaux et des systèmes d'information, le soutien à l'organisation et à la réalisation d'exercices de l'Union portant sur la sécurité des réseaux et des systèmes d'information et l'échange d'informations et de bonnes pratiques en matière de sensibilisation et de formation. L'ENISA devrait également participer à l'élaboration de lignes directrices pour la définition de critères sectoriels permettant d'établir l'ampleur de l'impact d'un incident.

([1]) Règlement (UE) nº 526/2013 du Parlement européen et du Conseil du 21 mai 2013 concernant l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) et abrogeant le règlement (CE) nº 460/2004 (JO L 165 du 18.6.2013, p. 41).

(39) Afin de promouvoir la sécurité renforcée des réseaux et des systèmes d'information, il convient que le groupe de coopération coopère, le cas échéant, avec les institutions, organes et organismes compétents de l'Union en vue d'échanger le savoir-faire et les bonnes pratiques et de fournir des conseils sur les aspects relatifs à la sécurité des réseaux et des systèmes d'information qui pourraient avoir une incidence sur leurs activités, dans le respect des dispositions en vigueur en matière d'échange d'informations restreintes. Dans sa coopération avec les services répressifs concernant les questions relatives à la sécurité des réseaux et des systèmes d'information susceptibles d'avoir une incidence sur leurs activités, le groupe de coopération devrait respecter les canaux d'information existants et les réseaux établis.

(40) Les informations relatives aux incidents s'avèrent de plus en plus précieuses pour le grand public et pour les entreprises, en particulier pour les petites et moyennes entreprises. Dans certains cas, ces informations sont déjà fournies par des sites internet au niveau national, dans la langue du pays et elles sont centrées principalement sur les incidents et événements ayant une dimension nationale. Étant donné que les entreprises exercent de plus en plus d'activités transfrontalières et que les citoyens recourent aux services en ligne, il convient que les informations concernant les incidents soient fournies sous forme agrégée au niveau de l'Union. Le secrétariat du réseau des CSIRT est encouragé à tenir à jour un site internet ou à héberger une page spéciale sur un site internet existant, mettant à la disposition du grand public des informations générales sur les principaux incidents qui sont survenus dans toute l'Union, en mettant l'accent sur les intérêts et les besoins des entreprises. Les CSIRT participant au réseau des CSIRT sont encouragés à fournir, à titre volontaire, les informations destinées à être publiées sur ce site internet sans que cela ne comporte d'informations confidentielles ou sensibles.

(41) Lorsque des informations sont considérées comme confidentielles conformément à la réglementation nationale ou de l'Union en matière de secret des affaires, cette confidentialité devrait être garantie lors de l'exécution des activités et de la réalisation des objectifs énoncés par la présente directive.

(42) Les exercices qui simulent des scénarios d'incidents en temps réel sont essentiels pour tester l'état de préparation et la coopération des États membres quant à la sécurité des réseaux et des systèmes d'information. Le cycle d'exercices CyberEurope coordonné par l'ENISA avec la participation des États membres est un outil utile pour réaliser des tests et établir des recommandations sur la manière dont la gestion d'incidents au niveau de l'Union devrait s'améliorer au fil du temps. Étant donné que les États membres ne sont pas actuellement tenus de programmer des exercices ni d'y participer, la création du réseau des CSIRT dans le cadre de la présente directive devrait leur permettre de prendre part à des exercices sur la base d'une planification précise et de choix stratégiques. Le groupe de coopération institué par la présente directive devrait examiner les décisions stratégiques concernant les exercices, en particulier, mais pas exclusivement, pour ce qui est de leur régularité et de la conception des scénarios. L'ENISA devrait, conformément à son mandat, soutenir l'organisation et la tenue d'exercices dans l'ensemble de l'Union en fournissant ses connaissances et ses conseils au groupe de coopération et au réseau des CSIRT.

(43) Étant donné que les problèmes de sécurité affectant les réseaux et les systèmes d'information ont une dimension mondiale, il est nécessaire de renforcer la coopération internationale pour améliorer les normes de sécurité et les échanges d'informations et pour promouvoir une approche commune au niveau mondial en ce qui concerne les problèmes de sécurité.

(44) C'est, dans une large mesure, aux opérateurs de services essentiels et aux fournisseurs de service numérique qu'incombe la responsabilité de garantir la sécurité des réseaux et des systèmes d'information. Il convient de promouvoir et de faire évoluer, au moyen d'exigences réglementaires appropriées et de pratiques sectorielles volontaires, une culture de la gestion des risques impliquant une analyse des risques et l'application de mesures de sécurité adaptées aux risques encourus. Il est aussi essentiel d'établir un socle commun de confiance pour que le groupe de coopération et le réseau des CSIRT fonctionnent réellement et que la coopération de la part de tous les États membres soit effective.

(45) La présente directive s'applique uniquement aux administrations publiques qui sont identifiées en tant qu'opérateurs de services essentiels. Il est donc de la responsabilité des États membres de garantir la sécurité des réseaux et des systèmes d'information des administrations publiques ne relevant pas du champ d'application de la présente directive.

(46) Parmi les mesures de gestion des risques figurent celles permettant d'identifier tous les risques d'incidents, de prévenir, de repérer et de gérer les incidents et d'en atténuer l'impact. La sécurité des réseaux et des systèmes d'information inclut la sécurité des données stockées, transmises et traitées.

(47) Les autorités compétentes devraient conserver la capacité d'adopter des lignes directrices relatives aux circonstances dans lesquelles les opérateurs de services essentiels sont tenus de notifier les incidents.

(48) De nombreuses entreprises dans l'Union s'appuient, pour délivrer leurs services, sur des fournisseurs de service numérique. Étant donné que certains services numériques pourraient représenter une ressource importante pour leurs utilisateurs, y compris des opérateurs de services essentiels, et que beaucoup de ces utilisateurs pourraient ne pas toujours disposer de solutions de rechange, il convient que la présente directive s'applique également aux fournisseurs de ce type de services. La sécurité, la continuité et la fiabilité du type de services numériques visés dans la présente directive sont essentielles pour le bon fonctionnement de nombreuses entreprises. La perturbation d'un tel service numérique pourrait empêcher la fourniture d'autres services qui s'appuient sur celui-ci et avoir dès lors une incidence sur des fonctions économiques et sociétales clés dans l'Union. De tels services numériques pourraient par conséquent revêtir une importance cruciale pour le bon fonctionnement des entreprises qui en dépendent et, par ailleurs, pour la participation de ces entreprises au marché intérieur et aux échanges transfrontaliers dans l'ensemble de l'Union. Les fournisseurs de service numérique relevant de la présente directive sont ceux qui sont considérés comme offrant des services numériques sur lesquels de nombreuses entreprises de l'Union s'appuient de plus en plus.

(49) Les fournisseurs de service numérique devraient garantir un niveau de sécurité à la hauteur du risque qui menace la sécurité des services numériques qu'ils proposent, compte tenu de l'importance de leurs services pour les activités d'autres entreprises au sein de l'Union. Dans la pratique, le degré de risque pour les opérateurs de services essentiels, qui sont souvent cruciaux pour le maintien de fonctions sociétales et économiques critiques, est plus élevé que pour les fournisseurs de service numérique. Par conséquent, les exigences en matière de sécurité imposées aux fournisseurs de service numérique devraient être moins strictes. Les fournisseurs de service numérique devraient rester libres de prendre les mesures qu'ils jugent appropriées pour gérer les risques qui menacent la sécurité de leurs réseaux et systèmes d'information. En raison du caractère transfrontalier de leurs activités, les fournisseurs de service numérique devraient faire l'objet d'une approche plus harmonisée au niveau de l'Union. La définition et la mise en œuvre de ces mesures devraient être facilitées au moyen d'actes d'exécution.

(50) Alors que les fabricants de matériel et les développeurs de logiciels ne sont pas des opérateurs de services essentiels ou des fournisseurs de service numérique, leurs produits renforcent la sécurité des réseaux et des systèmes d'information. Dès lors, ils jouent un rôle important en permettant aux opérateurs de services essentiels et aux fournisseurs de service numérique de sécuriser leurs réseaux et systèmes d'information. Ce matériel et ces logiciels font déjà l'objet de règles existantes sur la responsabilité du fait des produits.

(51) Les mesures techniques et organisationnelles imposées aux opérateurs de services essentiels et aux fournisseurs de service numérique ne devraient pas impliquer la conception, le développement ou la fabrication selon des modalités précises d'un produit commercial particulier relevant des technologies de l'information et de la communication.

(52) Les opérateurs de services essentiels et les fournisseurs de service numérique devraient garantir la sécurité des réseaux et des systèmes d'information qu'ils utilisent. Il s'agit principalement de réseaux et de systèmes d'information privés qui sont gérés par leurs propres services informatiques ou dont la gestion de la sécurité a été sous-traitée. Les exigences en matière de sécurité et de notification devraient s'appliquer aux opérateurs de services essentiels et aux fournisseurs de service numérique concernés, que la maintenance de leurs réseaux et systèmes d'information soit assurée en interne ou qu'elle soit sous-traitée.

(53) Pour éviter que la charge financière et administrative imposée aux opérateurs de services essentiels et aux fournisseurs de service numérique ne soit excessive, il convient que les exigences soient proportionnées aux risques que présentent le réseau et le système d'information concernés, compte tenu de l'état le plus avancé de la technique en ce qui concerne ces mesures. Dans le cas des fournisseurs de service numérique, ces exigences ne devraient pas être applicables aux microentreprises et aux petites entreprises.

(54) Les administrations publiques des États membres qui utilisent des services proposés par des fournisseurs de service numérique, notamment des services d'informatique en nuage, pourraient vouloir exiger de ces fournisseurs des mesures de sécurité supplémentaires allant au-delà de ce que ceux-ci proposeraient d'ordinaire dans le respect des exigences de la présente directive. Elles devraient pouvoir l'obtenir en imposant des obligations contractuelles.

(55) Les définitions des termes «place de marché en ligne», «moteur de recherche en ligne» et «services d'informatique en nuage» énoncées dans la présente directive servent aux fins spécifiques de la présente directive et sont sans préjudice d'autres instruments.

(56) La présente directive ne devrait pas empêcher les États membres d'adopter des mesures nationales obligeant les organismes du secteur public à fixer des exigences spécifiques en matière de sécurité lorsqu'ils passent des contrats pour des services d'informatique en nuage. De telles mesures nationales devraient s'appliquer à l'organisme du secteur public concerné et non au fournisseur de services d'informatique en nuage.

(57) Étant donné les différences fondamentales qui existent entre les opérateurs de services essentiels, notamment leur lien direct avec des infrastructures physiques, et les fournisseurs de service numérique, notamment le caractère transfrontalier de leurs activités, la présente directive devrait adopter une approche différenciée en ce qui concerne le niveau d'harmonisation à prévoir pour ces deux groupes d'entités. Pour les opérateurs de services essentiels, les États membres devraient pouvoir identifier les opérateurs concernés et imposer des exigences plus strictes que celles énoncées dans la présente directive. Les États membres ne devraient pas identifier les fournisseurs de service numérique dans la mesure où la présente directive devrait s'appliquer à tous les fournisseurs de service numérique relevant de son champ d'application. En outre, la présente directive et les actes d'exécution adoptés en vertu de celle-ci devraient garantir un niveau élevé d'harmonisation pour les fournisseurs de service numérique en ce qui concerne les exigences en matière de sécurité et de notification. Cela devrait permettre aux fournisseurs de service numérique de faire l'objet d'un traitement uniforme dans l'ensemble de l'Union, d'une manière proportionnée à la nature et à l'intensité du risque auquel ils pourraient être confrontés.

(58) La présente directive ne devrait pas empêcher les États membres d'imposer des exigences en matière de sécurité et de notification aux entités qui ne sont pas des fournisseurs de service numérique relevant du champ d'application de la présente directive, sans préjudice des obligations des États membres en vertu du droit de l'Union.

(59) Les autorités compétentes devraient veiller à préserver des canaux informels et dignes de confiance pour le partage d'informations. La divulgation d'informations sur les incidents signalés aux autorités compétentes devrait être le reflet d'un compromis entre l'intérêt, pour le public, d'être informé des menaces et les éventuelles conséquences néfastes, pour les opérateurs de services essentiels et les fournisseurs de service numérique signalant les incidents, en termes d'image comme sur le plan commercial. Lorsqu'ils mettent en œuvre les obligations de notification, les autorités compétentes et les CSIRT devraient être particulièrement attentifs à la nécessité de préserver la stricte confidentialité des informations sur les vulnérabilités des produits avant la publication des mises à jour de sécurité appropriées.

(60) Les fournisseurs de service numérique devraient être soumis à une surveillance a posteriori allégée et réactive, justifiée par la nature de leurs services et activités. L'autorité compétente concernée ne devrait dès lors intervenir que lorsqu'elle est informée, par exemple par le fournisseur de service numérique lui-même, par une autre autorité compétente, y compris une autorité compétente d'un autre État membre, ou par un utilisateur du service, d'éléments selon lesquels un fournisseur de service numérique ne satisfait pas aux exigences de la présente directive, notamment à la suite de la survenance d'un incident. L'autorité compétente devrait dès lors ne pas avoir d'obligation générale de surveiller les fournisseurs de service numérique.

(61) Les autorités compétentes devraient disposer des moyens nécessaires à l'exécution de leurs tâches, et notamment des pouvoirs leur permettant d'obtenir des informations suffisantes pour évaluer le niveau de sécurité des réseaux et des systèmes d'information.

(62) Un incident peut être le résultat d'activités criminelles, à propos desquelles la prévention, les enquêtes et les poursuites sont soutenues par la coordination et la coopération entre les opérateurs de services essentiels, les fournisseurs de service numérique, les autorités compétentes et les services répressifs. Lorsqu'il y a lieu de suspecter qu'un incident est lié à des activités criminelles graves au regard du droit de l'Union ou du droit national, les États membres devraient encourager les opérateurs de services essentiels et les fournisseurs de service numérique à signaler aux services répressifs compétents tout incident de ce type. Le cas échéant, il est souhaitable que la coordination entre les autorités compétentes et les services répressifs de différents États membres soit facilitée par le Centre européen de lutte contre la cybercriminalité (EC3) et l'ENISA.

(63) Dans de nombreux cas, des données à caractère personnel sont compromises à la suite d'incidents. Dans de telles circonstances, les autorités compétentes et les autorités chargées de la protection des données devraient coopérer et échanger des informations sur tous les aspects pertinents de la lutte contre toute atteinte aux données à caractère personnel à la suite d'incidents.

(64) La compétence dont relèvent les fournisseurs de service numérique devrait être attribuée à l'État membre dans lequel le fournisseur de service numérique concerné a son principal établissement dans l'Union, ce qui correspond en principe à l'endroit où il a son siège social dans l'Union. L'établissement suppose l'exercice effectif et réel d'une activité au moyen d'une installation stable. La forme juridique retenue pour un tel établissement, qu'il s'agisse d'une succursale ou d'une filiale ayant la personnalité juridique, n'est pas déterminante à cet égard.

Ce critère ne devrait pas dépendre du fait de savoir si les réseaux et systèmes d'information sont physiquement situés dans un lieu donné; la présence et l'utilisation de tels systèmes ne constituent pas en soi l'établissement principal et ne sont donc pas des critères permettant de déterminer l'établissement principal.

(65) Lorsqu'un fournisseur de service numérique, qui n'est pas établi dans l'Union, propose des services à l'intérieur de l'Union, il devrait désigner un représentant. Afin de déterminer si un tel fournisseur de service numérique propose des services dans l'Union, il convient d'examiner s'il apparaît qu'il envisage d'offrir des services à des personnes dans un ou plusieurs États membres. La seule accessibilité, dans l'Union, du site internet du fournisseur de service numérique ou d'un intermédiaire ou d'une adresse électronique et d'autres coordonnées ou encore l'utilisation d'une langue généralement utilisée dans le pays tiers où le fournisseur de service numérique est établi ne suffisent pas pour établir une telle intention. Cependant, des facteurs tels que l'utilisation d'une langue ou d'une monnaie généralement utilisées dans un ou plusieurs États membres avec la possibilité de commander des services dans cette autre langue ou la mention de clients ou d'utilisateurs qui se trouvent dans l'Union peuvent indiquer que le fournisseur de service numérique envisage d'offrir des services dans l'Union. Le représentant devrait agir pour le compte du fournisseur de service numérique et devrait pouvoir être contacté par les autorités compétentes ou les CSIRT. Le représentant devrait être expressément désigné par un mandat écrit du fournisseur de service numérique le chargeant d'agir en son nom pour remplir les obligations, y compris la notification des incidents, qui lui incombent en vertu de la présente directive.

(66) La normalisation des exigences en matière de sécurité est un processus guidé par le marché. Pour assurer l'application convergente des normes en matière de sécurité, les États membres devraient encourager le respect de normes précises ou la conformité à ces dernières afin de garantir un niveau élevé de sécurité des réseaux et des systèmes d'information au niveau de l'Union. L'ENISA devrait aider les États membres par la fourniture de conseils et de lignes directrices. À cette fin, il pourrait être utile d'élaborer des normes harmonisées, en se conformant au règlement (UE) nº 1025/2012 du Parlement européen et du Conseil ([1]).

(67) Les entités qui ne relèvent pas du champ d'application de la présente directive peuvent connaître des incidents ayant des conséquences importantes sur les services qu'elles fournissent. Lorsque ces entités estiment qu'il est dans l'intérêt public de notifier la survenance de tels incidents, elles devraient être en mesure de le faire à titre volontaire. Ces notifications devraient être traitées par l'autorité compétente ou le CSIRT lorsque leur traitement ne fait pas peser de charge disproportionnée ou inutile sur les États membres concernés.

(68) Afin d'assurer des conditions uniformes d'exécution de la présente directive, il convient de conférer des compétences d'exécution à la Commission pour fixer les modalités de procédure nécessaires au fonctionnement du groupe de coopération ainsi que les exigences en matière de sécurité et de notification applicables aux fournisseurs de service numérique. Ces compétences devraient être exercées en conformité avec le règlement (UE) nº 182/2011 du Parlement européen et du Conseil ([2]). Lorsqu'elle adopte des actes d'exécution liés aux modalités de procédure nécessaires pour le fonctionnement du groupe de coopération, il y a lieu que la Commission tienne le plus grand compte de l'avis de l'ENISA.

(69) Lorsqu'elle adopte des actes d'exécution concernant les exigences en matière de sécurité à imposer aux fournisseurs de service numérique, la Commission devrait tenir le plus grand compte de l'avis de l'ENISA et consulter les parties intéressées. De plus, la Commission est encouragée à prendre en compte les exemples suivants: en ce qui concerne la sécurité des systèmes et des installations: sécurité physique et environnementale, sécurité de l'approvisionnement, contrôle de l'accès aux réseaux et aux systèmes d'information et intégrité desdits réseaux et systèmes d'information; en ce qui concerne la gestion des incidents: procédures de gestion des incidents, dispositif de détection des incidents, compte-rendu et notification d'incidents; en ce qui concerne la gestion de la continuité des activités: stratégie en matière de continuité du service et plans d'urgence, dispositif de rétablissement après sinistre; et en ce qui concerne le suivi, le contrôle et les tests: politiques de surveillance et d'enregistrement, exercices de mise en œuvre de plans d'urgence, tests des réseaux et des systèmes d'information, évaluations de la sécurité et contrôle du respect des exigences.

(70) Dans la mise en œuvre de la présente directive, la Commission devrait communiquer comme il se doit avec les comités sectoriels et organismes pertinents établis au niveau de l'Union dans les domaines couverts par la présente directive.

([1]) Règlement (UE) nº 1025/2012 du Parlement européen et du Conseil du 25 octobre 2012 relatif à la normalisation européenne, modifiant les directives 89/686/CEE et 93/15/CEE du Conseil ainsi que les directives 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE et 2009/105/CE du Parlement européen et du Conseil et abrogeant la décision 87/95/CEE du Conseil et la décision nº 1673/2006/CE du Parlement européen et du Conseil (JO L 316 du 14.11.2012, p. 12).

([2]) Règlement (UE) nº 182/2011 du Parlement européen et du Conseil du 16 février 2011 établissant les règles et principes généraux relatifs aux modalités de contrôle par les États membres de l'exercice des compétences d'exécution par la Commission (JO L 55 du 28.2.2011, p. 13).

(71) La présente directive devrait être réexaminée périodiquement par la Commission, en consultation avec les parties prenantes intéressées, notamment en vue de déterminer s'il est nécessaire de la modifier pour tenir compte de l'évolution de la société, de la situation politique, des technologies ou de la situation des marchés.

(72) Le partage des informations sur les risques et incidents au sein du groupe de coopération et du réseau des CSIRT et le respect des exigences relatives à la notification des incidents aux autorités nationales compétentes ou aux CSIRT pourraient nécessiter le traitement de données à caractère personnel. Il convient que ce traitement respecte la directive 95/46/CE du Parlement européen et du Conseil [1] et le règlement (CE) nº 45/2001 du Parlement européen et du Conseil [2]. Dans l'application de la présente directive, le règlement (CE) nº 1049/2001 du Parlement européen et du Conseil [3] devrait s'appliquer, le cas échéant.

(73) Le Contrôleur européen de la protection des données a été consulté conformément à l'article 28, paragraphe 2, du règlement (CE) nº 45/2001 et a rendu son avis le 14 juin 2013 [4].

(74) Étant donné que l'objectif de la présente directive, qui vise à atteindre un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union, ne peut pas être atteint de manière suffisante par les États membres mais peut, en raison des effets de l'action, l'être mieux au niveau de l'Union, celle-ci peut prendre des mesures, conformément au principe de subsidiarité consacré à l'article 5 du traité sur l'Union européenne. Conformément au principe de proportionnalité tel qu'énoncé audit article, la présente directive n'excède pas ce qui est nécessaire pour atteindre cet objectif.

(75) La présente directive respecte les droits fondamentaux et observe les principes reconnus par la charte des droits fondamentaux de l'Union européenne et, en particulier, le droit au respect de la vie privée et des communications, le droit à la protection des données à caractère personnel, le droit à la liberté d'entreprise, le droit de propriété ainsi que le droit à un recours effectif et à un procès équitable. La présente directive devrait être mise en œuvre conformément à ces droits et principes,

ONT ADOPTÉ LA PRÉSENTE DIRECTIVE:

CHAPITRE I

DISPOSITIONS GÉNÉRALES

Article premier

Objet et champ d'application

1. La présente directive établit des mesures visant à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union afin d'améliorer le fonctionnement du marché intérieur.

2. À cette fin, la présente directive:

a) fixe des obligations à tous les États membres en ce qui concerne l'adoption d'une stratégie nationale en matière de sécurité des réseaux et des systèmes d'information;

b) institue un groupe de coopération afin de soutenir et faciliter la coopération stratégique et l'échange d'informations entre les États membres et de renforcer la confiance mutuelle;

c) institue un réseau des centres de réponse aux incidents de sécurité informatiques (ci-après dénommé «réseau des CSIRT») afin de contribuer au renforcement de la confiance entre les États membres et de promouvoir une coopération rapide et effective au niveau opérationnel;

---

[1] Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (JO L 281 du 23.11.1995, p. 31).

[2] Règlement (CE) nº 45/2001 du Parlement européen et du Conseil du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données (JO L 8 du 12.1.2001, p. 1).

[3] Règlement (CE) nº 1049/2001 du Parlement européen et du Conseil du 30 mai 2001 relatif à l'accès du public aux documents du Parlement européen, du Conseil et de la Commission (JO L 145 du 31.5.2001, p. 43).

[4] JO C 32 du 4.2.2014, p. 19.

d) établit des exigences en matière de sécurité et de notification pour les opérateurs de services essentiels et pour les fournisseurs de service numérique;

e) fixe des obligations aux États membres pour la désignation d'autorités nationales compétentes, de points de contact uniques et de CSIRT chargés de tâches liées à la sécurité des réseaux et des systèmes d'information.

3. Les exigences en matière de sécurité et de notification prévues par la présente directive ne s'appliquent pas aux entreprises soumises aux exigences énoncées aux articles 13 *bis* et 13 *ter* de la directive 2002/21/CE ni aux prestataires de services de confiance soumis aux exigences énoncées à l'article 19 du règlement (UE) nº 910/2014.

4. La présente directive est sans préjudice de la directive 2008/114/CE du Conseil ([1]) et des directives du Parlement européen et du Conseil 2011/93/UE ([2]) et 2013/40/UE ([3]).

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.

6. La présente directive est sans préjudice des mesures prises par les États membres pour préserver leurs fonctions étatiques essentielles, en particulier dans le but de préserver la sécurité nationale, notamment les mesures visant à protéger les informations dont la divulgation est considérée par les États membres comme contraire aux intérêts essentiels de leur sécurité, et de maintenir l'ordre public, en particulier pour permettre la détection des infractions pénales ainsi que les enquêtes et les poursuites en la matière.

7. Lorsqu'un acte juridique sectoriel de l'Union exige des opérateurs de services essentiels ou des fournisseurs de service numérique qu'ils assurent la sécurité de leurs réseaux et systèmes d'information ou qu'ils procèdent à la notification des incidents, à condition que les exigences en question aient un effet au moins équivalent à celui des obligations prévues par la présente directive, les dispositions de cet acte juridique sectoriel de l'Union s'appliquent.

Article 2

Traitement des données à caractère personnel

1. Le traitement de données à caractère personnel au titre de la présente directive est effectué conformément à la directive 95/46/CE.

2. Le traitement de données à caractère personnel par les institutions et organes de l'Union au titre de la présente directive est effectué conformément au règlement (CE) nº 45/2001.

Article 3

Harmonisation minimale

Sans préjudice de l'article 16, paragraphe 10, et des obligations qui leur incombent en vertu du droit de l'Union, les États membres peuvent adopter ou maintenir des dispositions en vue de parvenir à un niveau de sécurité plus élevé des réseaux et des systèmes d'information.

([1]) Directive 2008/114/CE du Conseil du 8 décembre 2008 concernant le recensement et la désignation des infrastructures critiques européennes ainsi que l'évaluation de la nécessité d'améliorer leur protection (JO L 345 du 23.12.2008, p. 75).

([2]) Directive 2011/93/UE du Parlement européen et du Conseil du 13 décembre 2011 relative à la lutte contre les abus sexuels et l'exploitation sexuelle des enfants, ainsi que la pédopornographie et remplaçant la décision-cadre 2004/68/JAI du Conseil (JO L 335 du 17.12.2011, p. 1).

([3]) Directive 2013/40/UE du Parlement européen et du Conseil du 12 août 2013 relative aux attaques contre les systèmes d'information et remplaçant la décision-cadre 2005/222/JAI du Conseil (JO L 218 du 14.8.2013, p. 8).

Article 4

Définitions

Aux fins de la présente directive, on entend par:

1) «réseau et système d'information»:

   a) un réseau de communications électroniques au sens de l'article 2, point a), de la directive 2002/21/CE;

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

   c) les données numériques stockées, traitées, récupérées ou transmises par les éléments visés aux points a) et b) en vue de leur fonctionnement, utilisation, protection et maintenance;

2) «sécurité des réseaux et des systèmes d'information»: la capacité des réseaux et des systèmes d'information de résister, à un niveau de confiance donné, à des actions qui compromettent la disponibilité, l'authenticité, l'intégrité ou la confidentialité de données stockées, transmises ou faisant l'objet d'un traitement, et des services connexes que ces réseaux et systèmes d'information offrent ou rendent accessibles;

3) «stratégie nationale en matière de sécurité des réseaux et des systèmes d'information»: un cadre prévoyant des objectifs et priorités stratégiques en matière de sécurité des réseaux et des systèmes d'information au niveau national;

4) «opérateur de services essentiels»: une entité publique ou privée dont le type figure à l'annexe II et qui répond aux critères énoncés à l'article 5, paragraphe 2;

5) «service numérique»: un service au sens de l'article 1er, paragraphe 1, point b), de la directive (UE) 2015/1535 du Parlement européen et du Conseil ([1]) dont le type figure dans la liste de l'annexe III;

6) «fournisseur de service numérique»: une personne morale qui fournit un service numérique;

7) «incident»: tout événement ayant un impact négatif réel sur la sécurité des réseaux et des systèmes d'information;

8) «gestion d'incident»: toutes les procédures utiles à la détection, à l'analyse et au confinement d'un incident et toutes les procédures utiles à l'intervention en cas d'incident;

9) «risque»: toute circonstance ou tout événement raisonnablement identifiable ayant un impact négatif potentiel sur la sécurité des réseaux et des systèmes d'information;

10) «représentant»: une personne physique ou morale établie dans l'Union qui est expressément désignée pour agir pour le compte d'un fournisseur de service numérique non établi dans l'Union, qui peut être contactée par une autorité nationale compétente ou un CSIRT à la place du fournisseur de service numérique concernant les obligations incombant audit fournisseur de service numérique en vertu de la présente directive;

11) «norme»: une norme au sens de l'article 2, point 1), du règlement (UE) no 1025/2012;

12) «spécification»: une spécification technique au sens de l'article 2, point 4), du règlement (UE) no 1025/2012;

13) «point d'échange internet» (IXP): une structure de réseau qui permet l'interconnexion de plus de deux systèmes autonomes indépendants, essentiellement aux fins de faciliter l'échange de trafic internet; un IXP n'assure l'interconnexion que pour des systèmes autonomes; un IXP n'exige pas que le trafic internet passant entre une paire quelconque de systèmes autonomes participants transite par un système autonome tiers, pas plus qu'il ne modifie ou n'altère par ailleurs un tel trafic;

14) «système de noms de domaine» (DNS): un système hiérarchique et distribué d'affectation de noms dans un réseau qui résout les questions liées aux noms de domaines;

([1]) Directive (UE) 2015/1535 du Parlement européen et du Conseil du 9 septembre 2015 prévoyant une procédure d'information dans le domaine des réglementations techniques et des règles relatives aux services de la société de l'information (JO L 241 du 17.9.2015, p. 1).

15) «fournisseur de services DNS»: une entité qui fournit des services DNS sur l'internet;

16) «registre de noms de domaine de haut niveau»: une entité qui administre et gère l'enregistrement de noms de domaine internet dans un domaine de haut niveau donné;

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 ([1]) 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.

Article 5

Identification des opérateurs de services essentiels

1. Au plus tard le 9 novembre 2018, pour chaque secteur et sous-secteur visé à l'annexe II, les États membres identifient les opérateurs de services essentiels ayant un établissement sur leur territoire.

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.

3. Aux fins du paragraphe 1, chaque État membre établit une liste des services visés au paragraphe 2, point a).

4. Aux fins du paragraphe 1, lorsqu'une entité fournit un service visé au paragraphe 2, point a), dans deux États membres ou plus, les États membres en question se consultent mutuellement. La consultation intervient avant que l'identification ne fasse l'objet d'une décision.

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.

6. Le rôle du groupe de coopération consiste, conformément aux tâches visées à l'article 11, à aider les États membres à suivre une approche cohérente dans le processus d'identification des opérateurs de services essentiels.

7. Aux fins du réexamen visé à l'article 23 et au plus tard le 9 novembre 2018, puis tous les deux ans, les États membres communiquent à la Commission les informations qui lui sont nécessaires pour évaluer la mise en œuvre de la présente directive, en particulier la cohérence des approches adoptées par les États membres pour l'identification des opérateurs de services essentiels. Ces informations comprennent au moins:

a) les mesures nationales permettant l'identification des opérateurs de services essentiels;

([1]) Directive 2013/11/UE du Parlement européen et du Conseil du 21 mai 2013 relative au règlement extrajudiciaire des litiges de consommation et modifiant le règlement (CE) nº 2006/2004 et la directive 2009/22/CE (directive relative au RELC) (JO L 165 du 18.6.2013, p. 63).

b) la liste des services visée au paragraphe 3;

c) le nombre d'opérateurs de services essentiels identifiés pour chaque secteur visé à l'annexe II et une indication de leur importance pour ce secteur;

d) les seuils, pour autant qu'ils existent, permettant de déterminer le niveau de l'offre pertinent en fonction du nombre d'utilisateurs tributaires de ce service visé à l'article 6, paragraphe 1, point a), ou de l'importance de cet opérateur de services essentiels particulier visée à l'article 6, paragraphe 1, point f).

Afin de contribuer à la transmission d'informations comparables, la Commission peut, en tenant le plus grand compte de l'avis de l'ENISA, adopter des lignes directrices techniques appropriées concernant les paramètres applicables aux informations visées dans le présent paragraphe.

Article 6

Effet disruptif important

1. Lorsque les États membres déterminent l'importance d'un effet disruptif visée à l'article 5, paragraphe 2, point c), ils prennent en compte au moins les facteurs transsectoriels suivants:

a) le nombre d'utilisateurs tributaires du service fourni par l'entité concernée;

b) la dépendance des autres secteurs visés à l'annexe II à l'égard du service fourni par cette entité;

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

d) la part de marché de cette entité;

e) la portée géographique eu égard à la zone susceptible d'être touchée par un incident;

f) l'importance que revêt l'entité pour garantir un niveau de service suffisant, compte tenu de la disponibilité de solutions de rechange pour la fourniture de ce service.

2. Afin de déterminer si un incident est susceptible d'avoir un effet disruptif important, les États membres prennent aussi en compte, le cas échéant, des facteurs sectoriels.

CHAPITRE II

CADRES NATIONAUX SUR LA SÉCURITÉ DES RÉSEAUX ET DES SYSTÈMES D'INFORMATION

Article 7

Stratégie nationale en matière de sécurité des réseaux et des systèmes d'information

1. Chaque État membre adopte une stratégie nationale en matière de sécurité des réseaux et des systèmes d'information qui définit les objectifs stratégiques et les mesures politiques et réglementaires appropriées en vue de parvenir à un niveau élevé de sécurité des réseaux et des systèmes d'information et de le maintenir et de couvrir au moins les secteurs visés à l'annexe II et les services visés à l'annexe III. La stratégie nationale en matière de sécurité des réseaux et des systèmes d'information porte, en particulier, sur les points suivants:

a) les objectifs et les priorités de la stratégie nationale en matière de sécurité des réseaux et des systèmes d'information;

b) un cadre de gouvernance permettant d'atteindre les objectifs et les priorités de la stratégie nationale en matière de sécurité des réseaux et des systèmes d'information, prévoyant notamment les rôles et les responsabilités des organismes publics et des autres acteurs pertinents;

c) l'inventaire des mesures en matière de préparation, d'intervention et de récupération, y compris la coopération entre les secteurs public et privé;

d) un aperçu des programmes d'éducation, de sensibilisation et de formation en rapport avec la stratégie nationale en matière de sécurité des réseaux et des systèmes d'information;

e) un aperçu des plans de recherche et de développement en rapport avec la stratégie nationale en matière de sécurité des réseaux et des systèmes d'information;

f) un plan d'évaluation des risques permettant d'identifier les risques;

g) une liste des différents acteurs concernés par la mise en œuvre de la stratégie nationale en matière de sécurité des réseaux et des systèmes d'information.

2. Les États membres peuvent demander à l'ENISA de leur prêter assistance dans l'élaboration de leur stratégie nationale en matière de sécurité des réseaux et des systèmes d'information.

3. Les États membres communiquent leur stratégie nationale en matière de sécurité des réseaux et des systèmes d'information à la Commission dans un délai de trois mois suivant son adoption. Dans ce cadre, les États membres peuvent exclure des éléments de la stratégie se rapportant à la sécurité nationale.

Article 8

Autorités nationales compétentes et point de contact unique

1. Chaque État membre désigne une ou plusieurs autorités nationales compétentes en matière de sécurité des réseaux et des systèmes d'information (ci-après dénommées «autorités compétentes»), couvrant au moins les secteurs visés à l'annexe II et les services visés à l'annexe III. Les États membres peuvent attribuer cette mission à une ou des autorités existantes.

2. Les autorités compétentes contrôlent l'application de la présente directive au niveau national.

3. Chaque État membre désigne un point de contact national unique en matière de sécurité des réseaux et des systèmes d'information (ci-après dénommé «point de contact unique»). Les États membres peuvent attribuer cette mission à une autorité existante. Lorsqu'un État membre désigne une seule autorité compétente, cette dernière fait aussi fonction de point de contact unique.

4. Le point de contact unique exerce une fonction de liaison pour assurer une coopération transfrontalière entre les autorités des États membres, ainsi qu'avec les autorités concernées des autres États membres, le groupe de coopération visé à l'article 11 et le réseau des CSIRT visé à l'article 12.

5. Les États membres veillent à ce que les autorités compétentes et les points de contact uniques disposent de ressources suffisantes pour pouvoir s'acquitter de leurs tâches de manière effective et efficace et atteindre ainsi les objectifs de la présente directive. Les États membres font en sorte que les représentants désignés pour siéger au sein du groupe de coopération puissent coopérer de manière effective, efficace et sûre.

6. En fonction des besoins et conformément au droit national, les autorités compétentes et le point de contact unique consultent les services répressifs nationaux compétents et les autorités nationales chargées de la protection des données et coopèrent avec eux.

7. Chaque État membre notifie sans tarder à la Commission la désignation de l'autorité compétente et du point de contact unique, les tâches qui leur sont confiées et toute modification ultérieure dans ce cadre. Chaque État membre rend publique la désignation de l'autorité compétente et du point de contact unique. La Commission publie la liste des points de contact uniques désignés.

Article 9

Centres de réponse aux incidents de sécurité informatique (CSIRT)

1. Chaque État membre désigne un ou plusieurs CSIRT, se conformant aux exigences énumérées à l'annexe I, point 1), couvrant au moins les secteurs visés à l'annexe II et les services visés à l'annexe III, chargés de la gestion des incidents et des risques selon un processus bien défini. Un CSIRT peut être établi au sein d'une autorité compétente.

2. Les États membres veillent à ce que les CSIRT disposent de ressources suffisantes pour pouvoir s'acquitter efficacement de leurs tâches énumérées à l'annexe I, point 2).

Les États membres veillent à ce que leurs CSIRT coopèrent de manière effective, efficace et sécurisée au sein du réseau des CSIRT visé à l'article 12.

3. Les États membres font en sorte que leurs CSIRT aient accès à une infrastructure d'information et de communication adaptée, sécurisée et résiliente au niveau national.

4. Les États membres informent la Commission des missions de leurs CSIRT ainsi que des principaux éléments de leurs processus de gestion des incidents.

5. Les États membres peuvent solliciter l'assistance de l'ENISA pour la mise en place des CSIRT nationaux.

Article 10

Coopération au niveau national

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.

CHAPITRE III

COOPÉRATION

Article 11

Groupe de coopération

1. Un groupe de coopération est institué aux fins de soutenir et de faciliter la coopération stratégique et l'échange d'informations entre les États membres et de renforcer la confiance, et de parvenir à un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union.

Le groupe de coopération exécute ses tâches en s'appuyant sur les programmes de travail bisannuels visés au paragraphe 3, deuxième alinéa.

2. Le groupe de coopération est composé de représentants des États membres, de la Commission et de l'ENISA.

Si besoin est, le groupe de coopération peut inviter des représentants des acteurs concernés à participer à ses travaux.

Le secrétariat est assuré par la Commission.

3. Le groupe de coopération est chargé des tâches suivantes:

a) fournir des orientations stratégiques pour les activités du réseau des CSIRT institué en vertu de l'article 12;

b) échanger les bonnes pratiques concernant l'échange d'informations sur les notifications d'incidents visé à l'article 14, paragraphes 3 et 5, et à l'article 16, paragraphes 3 et 6;

c) échanger les bonnes pratiques entre les États membres et, en coopération avec l'ENISA, aider les États membres à renforcer leurs capacités en matière de sécurité des réseaux et des systèmes d'information;

d) discuter des capacités et de l'état de préparation des États membres et, à titre volontaire, évaluer les stratégies nationales en matière de sécurité des réseaux et des systèmes d'information et l'efficacité des CSIRT, et identifier les bonnes pratiques;

e) échanger des informations et les bonnes pratiques en matière de sensibilisation et de formation;

f) échanger des informations et les bonnes pratiques en matière de recherche et de développement dans le domaine de la sécurité des réseaux et des systèmes d'information;

g) le cas échéant, procéder à des échanges d'expériences sur des questions relatives à la sécurité des réseaux et des systèmes d'information avec les institutions, organes ou organismes de l'Union concernés;

h) discuter des normes et des spécifications visées à l'article 19 avec les représentants des organismes de normalisation européens concernés;

i) recueillir des informations sur les bonnes pratiques en matière de risques et d'incidents;

j) examiner chaque année les rapports de synthèse visés à l'article 10, paragraphe 3, deuxième alinéa;

k) discuter du travail accompli en ce qui concerne les exercices relatifs à la sécurité des réseaux et des systèmes d'information, les programmes d'éducation et la formation, y compris le travail réalisé par l'ENISA;

l) avec l'assistance de l'ENISA, échanger les bonnes pratiques concernant l'identification, par les États membres, des opérateurs de services essentiels, y compris au regard des dépendances transfrontalières, en matière de risques et d'incidents;

m) discuter des modalités de signalement des notifications d'incidents visées aux articles 14 et 16.

Au plus tard le 9 février 2018, puis tous les deux ans, le groupe de coopération établit un programme de travail prévoyant les actions à entreprendre pour mettre en œuvre les objectifs et les tâches et qui est cohérent avec les objectifs de la présente directive.

4. Aux fins du réexamen visé à l'article 23 et au plus tard le 9 août 2018, puis tous les ans et demi, le groupe de coopération établit un rapport évaluant l'expérience acquise à la suite de la coopération stratégique visée au présent article.

5. La Commission adopte des actes d'exécution fixant les modalités de procédure nécessaires au fonctionnement du groupe de coopération. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 22, paragraphe 2.

Aux fins du premier alinéa, la Commission présente au comité visé à l'article 22, paragraphe 1, le premier projet d'acte d'exécution le 9 février 2017 au plus tard.

Article 12

Réseau des CSIRT

1. Afin de contribuer au renforcement de la confiance entre les États membres et de promouvoir une coopération opérationnelle rapide et effective, un réseau des CSIRT nationaux est établi.

2. Le réseau des CSIRT est composé de représentants des CSIRT des États membres et du CERT-UE. La Commission participe au réseau des CSIRT en qualité d'observateur. L'ENISA assure le secrétariat et soutient activement la coopération entre les CSIRT.

3. Le réseau des CSIRT est chargé des tâches suivantes:

a) échanger des informations sur les services, les opérations et les capacités de coopération des CSIRT;

b) à la demande du représentant d'un CSIRT d'un État membre susceptible d'être touché par un incident, échanger des informations non sensibles d'un point de vue commercial en rapport avec l'incident en question et les risques correspondants et en débattre; toutefois, un CSIRT d'un État membre peut refuser de contribuer à ce débat s'il existe un risque de porter atteinte à l'enquête sur l'incident;

c) échanger et mettre à disposition, à titre volontaire, des informations non confidentielles sur les différents incidents;

d) à la demande du représentant d'un CSIRT d'un État membre, discuter et, si possible, identifier une réponse coordonnée à un incident identifié qui relève de la juridiction de ce même État membre;

e) aider les États membres à faire face à des incidents transfrontaliers sur la base d'une assistance mutuelle volontaire;

f) débattre, étudier et identifier d'autres formes de coopération opérationnelle, notamment en rapport avec:

   i) les catégories de risques et d'incidents;

   ii) les alertes précoces;

   iii) l'assistance mutuelle;

   iv) les principes et modalités d'une coordination lorsque les États membres réagissent à des risques et incidents transfrontaliers;

g) informer le groupe de coopération des activités du réseau et des autres formes de coopération opérationnelle débattues en application du point f) et demander des orientations à cet égard;

h) étudier les enseignements tirés des exercices relatifs à la sécurité des réseaux et des systèmes d'information, y compris de ceux organisés par l'ENISA;

i) à la demande d'un CSIRT donné, étudier les capacités et l'état de préparation dudit CSIRT;

j) publier des lignes directrices afin de faciliter la convergence des pratiques opérationnelles en ce qui concerne l'application des dispositions du présent article relatives à la coopération opérationnelle.

4. Aux fins du réexamen visé à l'article 23 et au plus tard le 9 août 2018, puis tous les ans et demi, le réseau des CSIRT établit un rapport évaluant l'expérience acquise à la suite de la coopération opérationnelle visée au présent article, comprenant des conclusions et des recommandations. Ce rapport est aussi transmis au groupe de coopération.

5. Le réseau des CSIRT établit son propre règlement intérieur.

Article 13

Coopération internationale

L'Union peut, conformément à l'article 218 du traité sur le fonctionnement de l'Union européenne, conclure, avec des pays tiers ou des organisations internationales, des accords internationaux qui permettent et organisent leur participation à certaines activités du groupe de coopération. Ces accords tiennent compte de la nécessité d'assurer un niveau suffisant de protection des données.

CHAPITRE IV

SÉCURITÉ DES RÉSEAUX ET DES SYSTÈMES D'INFORMATION DES OPÉRATEURS DE SERVICES ESSENTIELS

Article 14

Exigences de sécurité et notification d'incidents

1. Les États membres veillent à ce que les opérateurs de services essentiels prennent les mesures techniques et organisationnelles nécessaires et proportionnées pour gérer les risques qui menacent la sécurité des réseaux et des systèmes d'information qu'ils utilisent dans le cadre de leurs activités. Ces mesures garantissent, pour les réseaux et les systèmes d'information, un niveau de sécurité adapté au risque existant, compte tenu de l'état des connaissances.

2. Les États membres veillent à ce que les opérateurs de services essentiels prennent les mesures appropriées en vue de prévenir les incidents qui compromettent la sécurité des réseaux et des systèmes d'information utilisés pour la fourniture de ces services essentiels ou d'en limiter l'impact, en vue d'assurer la continuité de ces services.

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. Cette notification n'accroît pas la responsabilité de la partie qui en est à l'origine.

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.

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.

Lorsque les circonstances le permettent, l'autorité compétente ou le CSIRT fournit à l'opérateur de services essentiels qui est à l'origine de la notification des informations utiles au suivi de sa notification, par exemple celles qui pourraient contribuer à une gestion efficace de l'incident.

À la demande de l'autorité compétente ou du CSIRT, le point de contact unique transmet les notifications visées au premier alinéa aux points de contact uniques des autres États membres touchés.

6. Après avoir consulté l'opérateur de services essentiels qui est à l'origine de la notification, l'autorité compétente ou le CSIRT peut informer le public concernant des incidents particuliers, lorsque la sensibilisation du public est nécessaire pour prévenir un incident ou gérer un incident en cours.

7. Les autorités compétentes, agissant de concert au sein du groupe de coopération, peuvent élaborer et adopter des lignes directrices relatives aux circonstances dans lesquelles les opérateurs de services essentiels sont tenus de notifier les incidents, y compris en ce qui concerne les paramètres permettant de déterminer l'ampleur de l'impact d'un incident au sens du paragraphe 4.

Article 15

Mise en œuvre et exécution

1. Les États membres veillent à ce que les autorités compétentes disposent des pouvoirs et des moyens nécessaires pour évaluer le respect, par les opérateurs de services essentiels, des obligations qui leur incombent en vertu de l'article 14, ainsi que les effets de ce respect sur la sécurité des réseaux et des systèmes d'information.

2. Les États membres veillent à ce que les autorités compétentes disposent des pouvoirs et des moyens leur permettant d'exiger des opérateurs de services essentiels qu'ils fournissent:

a) les informations nécessaires pour évaluer la sécurité de leurs réseaux et systèmes d'information, y compris les documents relatifs à leurs politiques de sécurité;

b) des éléments prouvant la mise en œuvre effective des politiques de sécurité, tels que les résultats d'un audit de sécurité exécuté par l'autorité compétente ou un auditeur qualifié et, dans ce dernier cas, qu'ils en mettent les résultats, y compris les éléments probants, à la disposition de l'autorité compétente.

Au moment de formuler une telle demande d'informations et de preuves, l'autorité compétente mentionne la finalité de la demande et précise quelles sont les informations exigées.

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.

4. Pour traiter des incidents donnant lieu à des violations des données à caractère personnel, l'autorité compétente coopère étroitement avec les autorités chargées de la protection des données.

CHAPITRE V

SÉCURITÉ DES RÉSEAUX ET DES SYSTÈMES D'INFORMATION DES FOURNISSEURS DE SERVICE NUMÉRIQUE

Article 16

Exigences de sécurité et notification d'incidents

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.

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. Cette notification n'accroît pas la responsabilité de la partie qui en est à l'origine.

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.

5. Lorsqu'un opérateur de services essentiels s'appuie sur un tiers fournisseur de service numérique pour la prestation d'un service essentiel au maintien de fonctions sociétales et économiques critiques, tout impact significatif sur la continuité des services essentiels en raison d'un incident touchant le fournisseur de service numérique est notifié par ledit opérateur.

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, 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.

7. Après avoir consulté le fournisseur de service numérique concerné, l'autorité compétente ou le CSIRT et, lorsque c'est approprié, les autorités ou les CSIRT des autres États membres concernés peuvent informer le public d'incidents particuliers ou imposer au fournisseur de service numérique de le faire, dans le cas où la sensibilisation du public est nécessaire pour prévenir un incident ou pour gérer un incident en cours, ou lorsque la divulgation de l'incident est dans l'intérêt public à d'autres égards.

8. La Commission adopte des actes d'exécution afin de compléter les éléments visés au paragraphe 1 et les paramètres énumérés au paragraphe 4 du présent article. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 22, paragraphe 2, au plus tard le 9 août 2017.

9. La Commission peut adopter des actes d'exécution fixant les formats et les procédures à appliquer pour respecter les exigences en matière de notification. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 22, paragraphe 2.

10. Sans préjudice de l'article 1er, paragraphe 6, les États membres n'imposent pas aux fournisseurs de service numérique d'autres exigences liées à la sécurité ou aux notifications.

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 ([1]).

([1]) Recommandation 2003/361/CE de la Commission du 6 mai 2003 concernant la définition des micro, petites et moyennes entreprises (JO L 124 du 20.5.2003, p. 36).

Article 17

Mise en œuvre et exécution

1. Les États membres veillent à ce que les autorités compétentes prennent des mesures, au besoin, dans le cadre de mesures de contrôle a posteriori, lorsque, selon les éléments communiqués, un fournisseur de service numérique ne satisfait pas aux exigences énoncées à l'article 16. Ces éléments peuvent être communiqués par une autorité compétente d'un autre État membre dans lequel le service est fourni.

2. Aux fins du paragraphe 1, les autorités compétentes disposent des pouvoirs et des moyens nécessaires pour imposer aux fournisseurs de service numérique:

a) de communiquer les informations nécessaires pour évaluer la sécurité de leurs réseaux et systèmes d'information, y compris les documents relatifs à leurs politiques de sécurité;

b) de corriger tout manquement aux obligations fixées à l'article 16.

3. Si un fournisseur de service numérique a son établissement principal ou un représentant dans un État membre alors que ses réseaux et systèmes d'information sont situés dans un ou plusieurs autres États membres, l'autorité compétente de l'État membre de l'établissement principal ou du représentant et les autorités compétentes de ces autres États membres coopèrent et se prêtent mutuellement assistance si nécessaire. Cette assistance et cette coopération peuvent porter sur les échanges d'informations entre les autorités compétentes concernées et sur les demandes de prise de mesures de contrôle visées au paragraphe 2.

Article 18

Compétence et territorialité

1. Aux fins de la présente directive, un fournisseur de service numérique est considéré comme relevant de la compétence de l'État membre dans lequel il a son établissement principal. Un fournisseur de service numérique est réputé 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.

3. La désignation d'un représentant par le fournisseur de service numérique est sans préjudice d'actions en justice qui pourraient être intentées contre le fournisseur de service numérique lui-même.

CHAPITRE VI

NORMALISATION ET NOTIFICATION VOLONTAIRE

Article 19

Normalisation

1. Afin de favoriser la convergence de la mise en œuvre de l'article 14, paragraphes 1 et 2, et de l'article 16, paragraphes 1 et 2, les États membres encouragent, sans imposer l'utilisation d'un type particulier de technologies ni créer de discrimination en faveur d'un tel type particulier de technologies, le recours à des normes et des spécifications européennes ou internationalement reconnues pour la sécurité des réseaux et des systèmes d'information.

2. L'ENISA, en collaboration avec les États membres, formule des avis et des lignes directrices relatives aux domaines techniques qui doivent être pris en considération en liaison avec le paragraphe 1 et relatives aux normes existantes, y compris les normes nationales des États membres, qui permettraient de couvrir ces domaines.

Article 20

Notification volontaire

1. Sans préjudice de l'article 3, les entités qui n'ont pas été identifiées en tant qu'opérateurs de services essentiels et qui ne sont pas des fournisseurs de service numérique peuvent notifier, à titre volontaire, les incidents ayant un impact significatif sur la continuité des services qu'elles fournissent.

2. Lorsqu'ils traitent des notifications, les États membres agissent conformément à la procédure énoncée à l'article 14. Les États membres peuvent traiter les notifications obligatoires en leur donnant la priorité par rapport aux notifications volontaires. Les notifications volontaires ne sont traitées que lorsque leur traitement ne fait pas peser de charge disproportionnée ou inutile sur les États membres concernés.

Une notification volontaire n'a pas pour effet d'imposer à l'entité qui est à l'origine de la notification des obligations auxquelles elle n'aurait pas été soumise si elle n'avait pas procédé à ladite notification.

CHAPITRE VII

DISPOSITIONS FINALES

Article 21

Sanctions

Les États membres fixent des règles relatives aux sanctions applicables en cas d'infraction aux dispositions nationales adoptées en vertu de la présente directive et prennent toutes les mesures nécessaires pour que ces règles soient appliquées. Les sanctions prévues sont effectives, proportionnées et dissuasives. Les États membres notifient ces règles et ces mesures à la Commission au plus tard le 9 mai 2018 et lui notifient sans retard toute modification ultérieure les concernant.

Article 22

Comité

1. La Commission est assistée par le comité de la sécurité des réseaux et des systèmes d'information. Ledit comité est un comité au sens du règlement (UE) nº 182/2011.

2. Lorsqu'il est fait référence au présent paragraphe, l'article 5 du règlement (UE) nº 182/2011 s'applique.

Article 23

Réexamen

1. Au plus tard le 9 mai 2019, la Commission présente au Parlement européen et au Conseil un rapport évaluant la cohérence de l'approche adoptée par les États membres pour identifier les opérateurs de services essentiels.

2. La Commission réexamine périodiquement le fonctionnement de la présente directive et en rend compte au Parlement européen et au Conseil. À cette fin et en vue de faire progresser la coopération stratégique et opérationnelle, la Commission tient compte des rapports du groupe de coopération et du réseau des CSIRT sur l'expérience acquise au niveau tant stratégique qu'opérationnel. Dans son réexamen, la Commission évalue en outre les listes figurant aux annexes II et III ainsi que la cohérence de l'identification des opérateurs de services essentiels et des services dans les secteurs visés à l'annexe II. Le premier rapport est présenté au plus tard le 9 mai 2021.

Article 24

Mesures transitoires

1. Sans préjudice de l'article 25 et afin d'offrir aux États membres des possibilités supplémentaires de coopération appropriée au cours de la période de transposition, le groupe de coopération et le réseau des CSIRT commencent à s'acquitter des tâches définies respectivement à l'article 11, paragraphe 3, et à l'article 12, paragraphe 3, au plus tard le 9 février 2017.

2. Au cours de la période comprise entre le 9 février 2017 et le 9 novembre 2018, et aux fins d'aider les États membres à adopter une approche cohérente dans le processus d'identification des opérateurs de services essentiels, le groupe de coopération discute du processus, ainsi que du contenu et du type des mesures nationales visant à identifier les opérateurs de services essentiels dans un secteur spécifique, conformément aux critères énoncés aux articles 5 et 6. Le groupe de coopération discute en outre, à la demande d'un État membre, des projets spécifiques de mesures nationales élaborés par cet État membre en vue d'identifier les opérateurs de services essentiels dans un secteur spécifique, conformément aux critères énoncés aux articles 5 et 6.

3. Au plus tard le 9 février 2017, et aux fins du présent article, les États membres assurent une représentation appropriée au sein du groupe de coopération et du réseau des CSIRT.

Article 25

Transposition

1. Les États membres adoptent et publient, au plus tard le 9 mai 2018, les dispositions législatives, réglementaires et administratives nécessaires pour se conformer à la présente directive. Ils en informent immédiatement la Commission.

Ils appliquent ces dispositions à partir du 10 mai 2018.

Lorsque les États membres adoptent ces dispositions, celles-ci contiennent une référence à la présente directive ou sont accompagnées d'une telle référence lors de leur publication officielle. Les modalités de cette référence sont arrêtées par les États membres.

2. Les États membres communiquent à la Commission le texte des dispositions essentielles de droit interne qu'ils adoptent dans le domaine régi par la présente directive.

Article 26

Entrée en vigueur

La présente directive entre en vigueur le vingtième jour suivant celui de sa publication au *Journal officiel de l'Union européenne*.

Article 27

Destinataires

Les États membres sont destinataires de la présente directive.

Fait à Strasbourg, le 6 juillet 2016.

Par le Parlement européen	*Par le Conseil*
Le président	*Le président*
M. SCHULZ	I. KORČOK

ANNEXE I

OBLIGATIONS ET TÂCHES DES CENTRES DE RÉPONSE AUX INCIDENTS DE SÉCURITÉ INFORMATIQUE (CSIRT)

Les obligations et tâches des CSIRT doivent être correctement et clairement définies sur la base d'une politique ou réglementation nationale. Elles comprennent les éléments suivants:

1) Obligations des CSIRT

   a) Les CSIRT doivent veiller à un niveau élevé de disponibilité de leurs services de communication en évitant les points uniques de défaillance et ils doivent disposer de plusieurs moyens pour être contactés et contacter autrui à tout moment. De plus, les canaux de communication doivent être clairement précisés et bien connus des partenaires et collaborateurs.

   b) Les locaux des CSIRT et les systèmes d'information utilisés doivent se trouver sur des sites sécurisés.

   c) Continuité des opérations:

      i) les CSIRT sont dotés d'un système approprié de gestion et de routage des demandes afin de faciliter les transferts;

      ii) les CSIRT sont dotés des effectifs adéquats afin de pouvoir garantir une disponibilité permanente;

      iii) les CSIRT s'appuient sur une infrastructure dont la continuité est garantie. À cette fin, des systèmes redondants et un espace de travail de secours sont disponibles.

   d) Les CSIRT ont la possibilité de participer, lorsqu'ils le souhaitent, aux réseaux de coopération internationale.

2) Tâches des CSIRT

   a) Les tâches des CSIRT comprennent au moins les éléments suivants:

      i) suivi des incidents au niveau national;

      ii) activation du mécanisme d'alerte précoce, diffusion de messages d'alerte, annonces et diffusion d'informations sur les risques et incidents auprès des parties intéressées;

      iii) intervention en cas d'incident;

      iv) analyse dynamique des risques et incidents et conscience situationnelle;

      v) participation au réseau des CSIRT.

   b) Les CSIRT établissent des relations de coopération avec le secteur privé.

   c) Pour faciliter la coopération, les CSIRT promeuvent l'adoption et l'utilisation de pratiques communes normalisées pour:

      i) les procédures de gestion des risques et incidents;

      ii) les systèmes de classification des incidents, risques et informations.

ANNEXE II

TYPES D'ENTITÉS AUX FINS DE L'ARTICLE 4, POINT 4)

Secteur	Sous-secteur	Type d'entités
1. Énergie	a) Électricité	— Entreprises d'électricité au sens de l'article 2, point 35), de la directive 2009/72/CE du Parlement européen et du Conseil [1], qui remplit la fonction de «fourniture» au sens de l'article 2, point 19), de ladite directive
		— Gestionnaires de réseau de distribution au sens de l'article 2, point 6), de la directive 2009/72/CE
		— Gestionnaires de réseau de transport au sens de l'article 2, point 4), de la directive 2009/72/CE
	b) Pétrole	— Exploitants d'oléoducs
		— Exploitants d'installations de production, de raffinage, de traitement, de stockage et de transport de pétrole
	c) Gaz	— Entreprises de fourniture au sens de l'article 2, point 8), de la directive 2009/73/CE du Parlement européen et du Conseil [2]
		— Gestionnaires de réseau de distribution au sens de l'article 2, point 6), de la directive 2009/73/CE
		— Gestionnaires de réseau de transport au sens de l'article 2, point 4), de la directive 2009/73/CE
		— Gestionnaires d'installation de stockage au sens de l'article 2, point 10), de la directive 2009/73/CE
		— Gestionnaires d'installation de GNL au sens de l'article 2, point 12), de la directive 2009/73/CE
		— Entreprises de gaz naturel au sens de l'article 2, point 1), de la directive 2009/73/CE
		— Exploitants d'installations de raffinage et de traitement de gaz naturel
2. Transports	a) Transport aérien	— Transporteurs aériens au sens de l'article 3, point 4), du règlement (CE) nº 300/2008 du Parlement européen et du Conseil [3]
		— Entités gestionnaires d'aéroports au sens de l'article 2, point 2), de la directive 2009/12/CE du Parlement européen et du Conseil [4], aéroports au sens de l'article 2, point 1), de ladite directive, y compris les aéroports du réseau central énumérés à l'annexe II, section 2, du règlement (UE) nº 1315/2013 du Parlement européen et du Conseil [5], et entités exploitant les installations annexes se trouvant dans les aéroports

Secteur	Sous-secteur	Type d'entités
		— Services du contrôle de la circulation aérienne au sens de l'article 2, point 1), du règlement (CE) nº 549/2004 du Parlement européen et du Conseil ([6])
	b) Transport ferroviaire	— Gestionnaires de l'infrastructure au sens de l'article 3, point 2), de la directive 2012/34/UE du Parlement européen et du Conseil ([7])
		— Entreprises ferroviaires au sens de l'article 3, point 1), de la directive 2012/34/UE, y compris les exploitants d'installations de services au sens de l'article 3, point 12), de la directive 2012/34/UE
	c) Transport par voie d'eau	— Sociétés de transport terrestre, maritime et côtier de passagers et de fret au sens de l'annexe I du règlement (CE) nº 725/2004 du Parlement européen et du Conseil ([8]), à l'exclusion des navires exploités à titre individuel par ces sociétés
		— Entités gestionnaires des ports au sens de l'article 3, point 1), de la directive 2005/65/CE du Parlement européen et du Conseil ([9]), y compris les installations portuaires au sens de l'article 2, point 11), du règlement (CE) nº 725/2004, ainsi que les entités exploitant des ateliers et des équipements à l'intérieur des ports
		— Exploitants de services de trafic maritime au sens de l'article 3, point o), de la directive 2002/59/CE du Parlement européen et du Conseil ([10])
	d) Transport routier	— Autorités routières au sens de l'article 2, point 12), du règlement délégué (UE) 2015/962 de la Commission ([11]), chargées du contrôle de gestion du trafic
		— Exploitants de systèmes de transport intelligents au sens de l'article 4, point 1), de la directive 2010/40/UE du Parlement européen et du Conseil ([12])
3. Banques		Établissements de crédit au sens de l'article 4, point 1), du règlement (UE) nº 575/2013 du Parlement européen et du Conseil ([13])
4. Infrastructures de marchés financiers		— Exploitants de plate-forme de négociation au sens de l'article 4, point 24), de la directive 2014/65/UE du Parlement européen et du Conseil ([14])
		— Contreparties centrales au sens de l'article 2, point 1), du règlement (UE) nº 648/2012 du Parlement européen et du Conseil ([15])
5. Secteur de la santé	Établissements de soins de santé (y compris les hôpitaux et les cliniques privées)	Prestataires de soins de santé au sens de l'article 3, point g), de la directive 2011/24/UE du Parlement européen et du Conseil ([16])

Secteur	Sous-secteur	Type d'entités
6. Fourniture et distribution d'eau potable		Fournisseurs et distributeurs d'eaux destinées à la consommation humaine au sens de l'article 2, point 1) a), de la directive 98/83/CE du Conseil ([17]), à l'exclusion des distributeurs pour lesquels la distribution d'eaux destinées à la consommation humaine ne constitue qu'une partie de leur activité générale de distribution d'autres produits et biens qui ne sont pas considérés comme des services essentiels
7. Infrastructures numériques		— IXP
		— Fournisseurs de services DNS
		— Registres de noms de domaines de haut niveau

([1]) Directive 2009/72/CE du Parlement européen et du Conseil du 13 juillet 2009 concernant des règles communes pour le marché intérieur de l'électricité et abrogeant la directive 2003/54/CE (JO L 211 du 14.8.2009, p. 55).
([2]) Directive 2009/73/CE du Parlement européen et du Conseil du 13 juillet 2009 concernant des règles communes pour le marché intérieur du gaz naturel et abrogeant la directive 2003/55/CE (JO L 211 du 14.8.2009, p. 94).
([3]) Règlement (CE) nº 300/2008 du Parlement européen et du Conseil du 11 mars 2008 relatif à l'instauration de règles communes dans le domaine de la sûreté de l'aviation civile et abrogeant le règlement (CE) nº 2320/2002 (JO L 97 du 9.4.2008, p. 72).
([4]) Directive 2009/12/CE du Parlement européen et du Conseil du 11 mars 2009 sur les redevances aéroportuaires (JO L 70 du 14.3.2009, p. 11).
([5]) Règlement (UE) nº 1315/2013 du Parlement européen et du Conseil du 11 décembre 2013 sur les orientations de l'Union pour le développement du réseau transeuropéen de transport et abrogeant la décision nº 661/2010/UE (JO L 348 du 20.12.2013, p. 1).
([6]) Règlement (CE) nº 549/2004 du Parlement européen et du Conseil du 10 mars 2004 fixant le cadre pour la réalisation du ciel unique européen («règlement-cadre») (JO L 96 du 31.3.2004, p. 1).
([7]) Directive 2012/34/UE du Parlement européen et du Conseil du 21 novembre 2012 établissant un espace ferroviaire unique européen (JO L 343 du 14.12.2012, p. 32).
([8]) Règlement (CE) nº 725/2004 du Parlement européen et du Conseil du 31 mars 2004 relatif à l'amélioration de la sûreté des navires et des installations portuaires (JO L 129 du 29.4.2004, p. 6).
([9]) Directive 2005/65/CE du Parlement européen et du Conseil du 26 octobre 2005 relative à l'amélioration de la sûreté des ports (JO L 310 du 25.11.2005, p. 28).
([10]) Directive 2002/59/CE du Parlement européen et du Conseil du 27 juin 2002 relative à la mise en place d'un système communautaire de suivi du trafic des navires et d'information, et abrogeant la directive 93/75/CEE du Conseil (JO L 208 du 5.8.2002, p. 10).
([11]) Règlement délégué (UE) 2015/962 de la Commission du 18 décembre 2014 complétant la directive 2010/40/UE du Parlement européen et du Conseil en ce qui concerne la mise à disposition, dans l'ensemble de l'Union, de services d'informations en temps réel sur la circulation (JO L 157 du 23.6.2015, p. 21).
([12]) Directive 2010/40/UE du Parlement européen et du Conseil du 7 juillet 2010 concernant le cadre pour le déploiement de systèmes de transport intelligents dans le domaine du transport routier et d'interfaces avec d'autres modes de transport (JO L 207 du 6.8.2010, p. 1).
([13]) Règlement (UE) nº 575/2013 du Parlement européen et du Conseil du 26 juin 2013 concernant les exigences prudentielles applicables aux établissements de crédit et aux entreprises d'investissement et modifiant le règlement (UE) nº 648/2012 (JO L 176 du 27.6.2013, p. 1).
([14]) Directive 2014/65/UE du Parlement européen et du Conseil du 15 mai 2014 concernant les marchés d'instruments financiers et modifiant la directive 2002/92/CE et la directive 2011/61/UE (JO L 173 du 12.6.2014, p. 349).
([15]) Règlement (UE) nº 648/2012 du Parlement européen et du Conseil du 4 juillet 2012 sur les produits dérivés de gré à gré, les contreparties centrales et les référentiels centraux (JO L 201 du 27.7.2012, p. 1).
([16]) Directive 2011/24/UE du Parlement européen et du Conseil du 9 mars 2011 relative à l'application des droits des patients en matière de soins de santé transfrontaliers (JO L 88 du 4.4.2011, p. 45).
([17]) Directive 98/83/CE du Conseil du 3 novembre 1998 relative à la qualité des eaux destinées à la consommation humaine (JO L 330 du 5.12.1998, p. 32).

ANNEXE III

TYPES DE SERVICES NUMÉRIQUES AUX FINS DE L'ARTICLE 4, POINT 5)

1. Place de marché en ligne
2. Moteurs de recherche en ligne
3. Service d'informatique en nuage

FICHE D'EVALUATION D'IMPACT

Coordonnées du projet

Intitulé du projet :	**Avant-projet de loi portant transposition de la directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union et modifiant 1. la loi du 23 juillet 2016 portant création d'un Haut-Commissariat à la Protection nationale et 2. la loi modifiée du 20 avril 2009 portant création du Centre des technologies de l'information de l'Etat**
Ministère initiateur :	**Ministère d'Etat**
Auteur(s) :	**Elisabeth Wirion**
Téléphone :	**247-88912**
Courriel :	**elisabeth.wirion@hcpn.etat.lu**
Objectif(s) du projet :	**Le projet de loi vise à transposer la directive (UE) 2016/1148.**
Autre(s) Ministère(s)/Organisme(s)/Commune(s)impliqué(e)(s) :	
L'élaboration du projet de loi a fait l'objet d'une collaboration étroite entre le Haut-Commissariat à la Protection nationale (HCPN), l'Institut luxembourgeois de régulation et la Commission de surveillance du secteur financier. En plus, le projet a été présenté au comité interministériel de coordination en matière de cyberprévention et de cybersécurité qui regroupe des représentants du Ministère de l'Economie, du Centre des technologies de l'information de l'Etat, de la Direction de la défense, du Service des médias et des communications, du Service de renseignement de l'Etat, du G.I.E. Security made in Luxembourg, de l'Agence nationale de la sécurité des systèmes d'information, du CERT Gouvernemental et du HCPN.	
Date :	**10.4.2018**

Mieux légiférer

1. Partie(s) prenante(s) (organismes divers, citoyens, …) consultée(s) : Oui ☐ Non ☒
   Si oui, laquelle/lesquelles :
   Remarques/Observations :

2. Destinataires du projet :
   – Entreprises/Professions libérales : Oui ☒ Non ☐
   – Citoyens : Oui ☐ Non ☒
   – Administrations : Oui ☐ Non ☒

3. Le principe « Think small first » est-il respecté ? Oui ☒ Non ☐ N.a.[1] ☐
   (c.-à-d. des exemptions ou dérogations sont-elles prévues suivant la taille de l'entreprise et/ou son secteur d'activité ?)
   Remarques/Observations :
   Le chapitre 4 du projet ne s'applique pas aux microentreprises et petites entreprises telles que définies dans le règlement grand-ducal du 16 mars 2005 portant adaptation de la définition des micro, petites et moyennes entreprises.

1 N.a. : non applicable.

4. Le projet est-il lisible et compréhensible pour le destinataire ? Oui ☒ Non ☐
   Existe-t-il un texte coordonné ou un guide pratique, mis à jour et publié d'une façon régulière ? Oui ☐ Non ☒
   Remarques/Observations :

5. Le projet a-t-il saisi l'opportunité pour supprimer ou simplifier des régimes d'autorisation et de déclaration existants, ou pour améliorer la qualité des procédures ? Oui ☐ Non ☒
   Remarques/Observations :

6. Le projet contient-il une charge administrative[2] pour le(s) destinataire(s) ? (un coût imposé pour satisfaire à une obligation d'information émanant du projet ?) Oui ☒ Non ☐
   Si oui, quel est le coût administratif[3] approximatif total ? (nombre de destinataires x coût administratif par destinataire)
   Divers coûts sont à supporter par les opérateurs de services essentiels (OSE) et les fournisseurs de service numérique (FSN) afin de répondre aux exigences posées par le projet (obligation de notifier les incidents à l'autorité compétente, obligation de prévenir et de gérer les incidents).

7. a) Le projet prend-il recours à un échange de données interadministratif (national ou international) plutôt que de demander l'information au destinataire ? Oui ☐ Non ☒ N.a. ☐
   Si oui, de quelle(s) donnée(s) et/ou administration(s) s'agit-il ?
   b) Le projet en question contient-il des dispositions spécifiques concernant la protection des personnes à l'égard du traitement des données à caractère personnel[4] ? Oui ☒ Non ☐ N.a. ☐
   Si oui, de quelle(s) donnée(s) et/ou administration(s) s'agit-il ?
   Afin de traiter les incidents donnant lieu à des violations des données à caractère personnel, l'autorité compétente concernée collaborera avec la Commission nationale pour la protection des données.

8. Le projet prévoit-il :
   – une autorisation tacite en cas de non-réponse de l'administration ? Oui ☐ Non ☒ N.a. ☐
   – des délais de réponse à respecter par l'administration ? Oui ☐ Non ☒ N.a. ☐
   – le principe que l'administration ne pourra demander des informations supplémentaires qu'une seule fois ? Oui ☐ Non ☒ N.a. ☐

9. Y a-t-il une possibilité de regroupement de formalités et/ou de procédures (p. ex. prévues le cas échéant par un autre texte) ? Oui ☐ Non ☒ N.a. ☐
   Si oui, laquelle :

---

2 Il s'agit d'obligations et de formalités administratives imposées aux entreprises et aux citoyens, liées à l'exécution, l'application ou la mise en oeuvre d'une loi, d'un règlement grand-ducal, d'une application administrative, d'un règlement ministériel, d'une circulaire, d'une directive, d'un règlement UE ou d'un accord international prévoyant un droit, une interdiction ou une obligation.

3 Coût auquel un destinataire est confronté lorsqu'il répond à une obligation d'information inscrite dans une loi ou un texte d'application de celle-ci (exemple: taxe, coût de salaire, perte de temps ou de congé, coût de déplacement physique, achat de matériel, etc.).

4 Loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel (www.cnpd.lu)

10. En cas de transposition de directives communautaires, le principe « la directive, rien que la directive » est-il respecté ? Oui ☒ Non ☐ N.a. ☐
    Sinon, pourquoi ?

11. Le projet contribue-t-il en général à une :
    a) simplification administrative, et/ou à une Oui ☐ Non ☒
    b) amélioration de la qualité réglementaire ? Oui ☐ Non ☒
    Remarques/Observations :

12. Des heures d'ouverture de guichet, favorables et adaptées aux besoins du/des destinataire(s), seront-elles introduites ? Oui ☐ Non ☒ N.a. ☐

13. Y a-t-il une nécessité d'adapter un système informatique auprès de l'Etat (e-Government ou application back-office) ? Oui ☒ Non ☐
    Si oui, quel est le délai pour disposer du nouveau système ?
    Il est envisagé de mettre en place une plateforme de notification unique.

14. Y a-t-il un besoin en formation du personnel de l'administration concernée ? Oui ☒ Non ☐ N.a. ☐
    Si oui, lequel ?
    L'ILR sera l'autorité compétente concernée pour des secteurs qui lui sont étrangers à l'heure actuelle. Ainsi, un besoin en formation pourrait s'imposer.
    Remarques/Observations :

Egalité des chances

15. Le projet est-il :
    – principalement centré sur l'égalité des femmes et des hommes ? Oui ☐ Non ☒
    – positif en matière d'égalité des femmes et des hommes ? Oui ☐ Non ☒
      Si oui, expliquez de quelle manière :
    – neutre en matière d'égalité des femmes et des hommes ? Oui ☒ Non ☐
      Si oui, expliquez pourquoi :
    – négatif en matière d'égalité des femmes et des hommes ? Oui ☐ Non ☒
      Si oui, expliquez de quelle manière :

16. Y a-t-il un impact financier différent sur les femmes et les hommes ? Oui ☐ Non ☒ N.a. ☐
    Si oui, expliquez de quelle manière :

Directive « services »

17. Le projet introduit-il une exigence relative à la liberté d'établissement soumise à évaluation[5] ? Oui ☐ Non ☒ N.a. ☐
    Si oui, veuillez annexer le formulaire A, disponible au site Internet du Ministère de l'Economie et du Commerce extérieur :
    www.eco.public.lu/attributions/dg2/d_consommation/d_march_int_rieur/Services/index.html

5 Article 15, paragraphe 2 de la directive « services » (cf. Note explicative, p. 10-11)

18. Le projet introduit-il une exigence relative à la libre prestation de services transfrontaliers[6] ? Oui ☐ Non ☒ N.a. ☐

Si oui, veuillez annexer le formulaire B, disponible au site Internet du Ministère de l'Economie et du Commerce extérieur :

www.eco.public.lu/attributions/dg2/d_consommation/d_march_int_rieur/Services/index.html

6 Article 16, paragraphe 1, troisième alinéa et paragraphe 3, première phrase de la directive « services » (cf. Note explicative, p. 10-11)

Impression: CTIE – Division Imprimés et Fournitures de bureau