JOURNAL OFFICIEL

DU GRAND-DUCHÉ DE LUXEMBOURG

MÉMORIAL A

N° 372 du 31 mai 2019

Loi du 28 mai 2019 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 européenne et modifiant

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

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

Notre Conseil d'État entendu ;

De l'assentiment de la Chambre des Députés ;

Vu la décision de la Chambre des députés du 15 mai 2019 et celle du Conseil d'État du 21 mai 2019 portant qu'il n'y a pas lieu à second vote ;

Avons ordonné et ordonnons :

Chapitre 1er - Définitions et champ d'application

Art. 1er.

(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.

Art. 2.

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 lettres 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 dont le type figure en annexe et qui répond aux critères énoncés à l'article 7, paragraphe 2 ;

4° « Service numérique » : un service au sens de l'article 1er, paragraphe 1er, lettre 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 européenne qui est expressément désignée pour agir pour le compte d'un fournisseur de service numérique non établi dans l'Union européenne ;

10° « Norme » : une norme au sens de l'article 2, point 1, du règlement (UE) n° 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 n° 1673/2006/CE du Parlement européen et du Conseil ;

11° « Spécification » : une spécification technique au sens de l'article 2, point 4, du règlement (UE) n° 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 n° 1673/2006/CE du Parlement européen et du Conseil ;

12° « Point d'échange internet », ci-après « 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 », ci-après « 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 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° « CERT Gouvernemental » : Centre de traitement des urgences informatiques, tel que défini à l'arrêté grand-ducal du 9 mai 2018 déterminant l'organisation et les attributions du Centre de traitement des urgences informatiques, dénommé « CERT Gouvernemental » ;

20° « CIRCL » : Computer Incident Response Center Luxembourg, opéré par le groupement d'intérêt économique Security Made in Lëtzebuerg ;
21° « CSIRT » : centre de réponse aux incidents de sécurité informatiques ;
22° « Groupe de coopération » : groupe 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 européenne ;
23° « Réseau des CSIRT » : groupe institué aux fins de contribuer au renforcement de la confiance entre les États membres et de promouvoir une coopération opérationnelle rapide et effective ;
24° « Point de contact national unique » : autorité qui 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 et le réseau des CSIRT.

Chapitre 2 - Autorités compétentes concernées et point de contact national unique

Art. 3.

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 établissements de crédit 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.

L'obligation au secret professionnel prévue par l'article 16 de la loi modifiée du 23 décembre 1998 portant création d'une commission de surveillance du secteur financier et l'article 15 de la loi modifiée du 30 mai 2005 portant : 1) organisation de l'Institut Luxembourgeois de Régulation ; 2) modification de la loi modifiée du 22 juin 1963 fixant le régime des traitements des fonctionnaires de l'État ne fait pas obstacle à l'échange d'informations entre autorités compétentes.

Art. 4.

L'ILR constitue le point de contact national unique en matière de sécurité des réseaux et des systèmes d'information.

Art. 5.

L'ILR bénéficie d'une contribution financière à charge du budget de l'État afin de couvrir l'intégralité des frais de fonctionnement qui résultent de l'exercice des missions prévues par la présente loi.

Art. 6.

Dans la mesure nécessaire à l'accomplissement de leur mission en vertu de la présente loi, les autorités compétentes et le point de contact national unique consultent les services répressifs nationaux compétents et les autorités nationales chargées de la protection des données et coopèrent avec eux.

L'obligation au secret professionnel prévue par l'article 16 de la loi modifiée du 23 décembre 1998 portant création d'une Commission de surveillance du secteur financier et l'article 15 de la loi modifiée du 30 mai 2005 portant : 1) organisation de l'Institut Luxembourgeois de Régulation ; 2) modification de la loi modifiée du 22 juin 1963 fixant le régime des traitements des fonctionnaires de l'État ne fait pas obstacle à cette coopération.

Chapitre 3 - Opérateurs de services essentiels

Art. 7.

(1) Tombent sous le champ d'application de la présente loi, les opérateurs de services essentiels ayant un établissement sur le territoire luxembourgeois.

(2) 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.

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

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.

(4) La liste des services essentiels est fixée par l'autorité compétente concernée par voie de règlement.

(5) Lorsqu'une entité fournit un service visé au paragraphe 2, point 1, dans un autre État membre, l'autorité compétente concernée consulte l'autorité compétente de l'autre État membre. La consultation intervient avant que l'identification ne fasse l'objet d'une décision.

Art. 8.

(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 par voie de règlement.

(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 1er et 2 sont notifiées à l'autorité compétente concernée. Les modalités de cette notification, le format et le délai, sont déterminées par l'autorité compétente concernée par voie de règlement.

(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, en particulier, 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, par voie de règlement, les paramètres, 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 États membres touchés si l'incident est susceptible d'avoir un impact significatif sur la continuité des services essentiels dans ces États membres. Sur demande de l'autorité

compétente concernée, ce signalement est effectué par le point de contact national unique qui transmettra la notification aux points de contact nationaux des autres États membres touchés. Ce faisant, l'autorité compétente concernée doit 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.

(7) Une fois par an, l'autorité compétente concernée transmet au point de contact national 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 national 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. 9.

(1) À 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 ces violations.

Chapitre 4 - Fournisseurs de service numérique

Art. 10.

(1) Tombent dans 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 européenne 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 la recommandation 2003/361/CE de la Commission du 6 mai 2003 concernant la définition des micro, petites et moyennes entreprises.

Art. 11.

(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 européenne, 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 européenne, 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 européenne. Les modalités de cette notification, le format et le délai, sont déterminés par l'autorité compétente concernée par voie de règlement. 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, en particulier, 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 États membres ou plus, l'autorité compétente concernée peut informer les autres États membres touchés. Ce faisant, l'autorité compétente concernée doit 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 national 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 national 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 États membres concernés peuvent informer le public d'incidents particuliers ou imposer au fournisseur de service numérique de le faire, dans le cas où la sensibilisation du public est nécessaire pour prévenir un incident ou pour gérer un incident en cours, ou lorsque la divulgation de l'incident est dans l'intérêt public à d'autres égards.

Art. 12.

(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 11 ;
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 États membres, les autorités compétentes concernées luxembourgeoises et les autorités compétentes de ces autres États membres coopèrent étroitement et se prêtent mutuellement assistance dans la mesure nécessaire à l'application de la présente loi.

L'obligation au secret professionnel prévue par l'article 16 de la loi modifiée du 23 décembre 1998 portant création d'une Commission de surveillance du secteur financier et l'article 15 de la loi modifiée du 30 mai 2005 portant : 1) organisation de l'Institut Luxembourgeois de Régulation ; 2) modification de la loi modifiée du 22 juin 1963 fixant le régime des traitements des fonctionnaires de l'État ne fait pas obstacle à cette coopération.

Chapitre 5 - Notification volontaire

Art. 13.

(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 8. 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'autorité 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. 14.

(1) Lorsque l'autorité compétente concernée constate une violation des obligations prévues par les articles 8, 9, 11 et 12 ou par des mesures prises en exécution de la présente 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.

(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. À 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, des domaines et de la TVA.

Chapitre 7 - Dispositions modificatives

Art. 15.

À l'article 2, lettre y), de la loi modifiée du 20 avril 2009 portant création du Centre des technologies de l'information de l'État, 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. 16.

La loi du 23 juillet 2016 portant création d'un Haut-Commissariat à la Protection nationale est modifiée comme suit :

1° À l'article 2, point 4, le point final est remplacé par un point-virgule et il est inséré à la suite du point 4 un nouveau point 5, libellé 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° À l'article 3, paragraphe 1er, lettre b), il est ajouté un point 4, libellé comme suit :

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

3° À l'article 8, paragraphe 1er, les termes « l'article 5 » sont remplacés par les termes « l'article 4 » ;
4° Après l'article 9, il est inséré un nouveau chapitre 4*bis*, libellé comme suit :

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

Art. 9*bis*.

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. 17.

La présente loi entre en vigueur le premier jour du deuxième mois qui suit celui de 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.

Le Premier Ministre,
Ministre d'État,
Ministre des Communications et des Médias,
Xavier Bettel

Le Ministre des Finances,
Pierre Gramegna

Palais de Luxembourg, le 28 mai 2019.
Henri

Doc. parl. 7314 ; sess. ord. 2017-2018 et 2018-2019 ; Dir. (UE) 2016/1148.

ANNEXE

Types d'entités aux fins de l'article 2, point 3

Secteur	Sous-secteur	Type d'entités
1. Énergie	a) Électricité	- 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
		- 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

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) n° 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 n° 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 31 mars 2004 relatif à l'amélioration de la sûreté des navires et des installations portuaires, 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
	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. Établissements de crédit		- Établissements 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 1er, point 43, de la loi du 30 mai 2018 relative aux marchés d'instruments financiers
		- 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	Établissements 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 modifiée du 24 juillet 2014 relative aux droits et obligations du patient
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