N° 7314[8]

CHAMBRE DES DEPUTES

Session ordinaire 2018-2019

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 européenne et modifiant :

1° la loi modifiée du 20 avril 2009 portant création du Centre des technologies de l'Information de l'Etat et

2° la loi du 23 juillet 2016 portant création d'un Haut-Commissariat à la Protection nationale

* * *

RAPPORT DE LA COMMISSION DE LA DIGITALISATION, DES MEDIAS ET DES COMMUNICATIONS

(7.5.2019)

La commission se compose de M. Guy ARENDT, Président, M. Eugène BERGER, Rapporteur, Mme Diane ADEHM, M. Carlo BACK, Mme Djuna BERNARD, MM. Sven CLEMENT, Franz FAYOT et Marc HANSEN, Mme Carole HARTMANN, M. Marc LIES, Mmes Octavie MODERT et Lydia MUTSCH, M. Roy REDING, Mme Viviane REDING, M. Serge WILMES, Membres.

*

I. ANTECEDENTS

Le projet de loi n° 7314 (PL 7314) a été déposé à la Chambre des Députés le 6 juin 2018 par M. le Premier Ministre, Ministre d'Etat.

Renvoyé à l'époque – en date du 7 juin 2018 – à la Commission de l'Enseignement supérieur, de la Recherche, des Médias, des Communications et de l'Espace[1] de la Chambre, le PL 7314 fut avisé le 10 juillet 2018 par le Conseil d'Etat, imité en cela le 29 août 2018 par la Chambre des Métiers.

En date du 2 octobre 2018, la Chambre fut, moyennant demande de la part de M. le Premier Ministre, Ministre d'Etat, Ministre des Communications et des Médias, saisi de 35 amendements gouvernementaux relatifs au dit projet, non sans que celui-ci ait entretemps changé d'intitulé[2].

Le 27 novembre 2018, ces 35 amendements gouvernementaux firent l'objet d'un avis complémentaire de la Haute Corporation alors qu'en date du 13 décembre 2018, le PL 7314 fut officiellement renvoyé en Commission de la Digitalisation, des Médias et des Communications de la Chambre.

S'ensuivit l'élaboration en date du 14 novembre 2018 d'un avis de la Chambre de Commerce sur le projet de loi et les amendements gouvernementaux y relatifs avant que les membres de la commission parlementaire compétente de la Chambre, réunis le 12 mars 2019, ne décident d'adopter 4 amendements

---

1 Suite à l'assermentation du nouveau Gouvernement par S.A.R. le Grand-Duc en date du 5 décembre 2018, la Commission de l'Enseignement supérieur, de la Recherche, des Médias, des Communications et de l'Espace fut rebaptisée en Commission de la Digitalisation, des Médias et des Communications.

2 Dans son avis du 11 juillet 2017, le Conseil d'Etat avait en effet conseillé de citer dans le libellé du projet de loi en question les actes à modifier dans l'ordre chronologique, en commençant par le plus ancien.

parlementaires qui firent l'objet, en date du 26 avril 2019, d'un deuxième avis complémentaire de la part de la Haute Corporation.

Comme le Conseil d'Etat ne trouva rien à redire aux 4 amendements parlementaires dont il fut saisi ni à une version rectifiée de l'amendement n°4 qui lui fut envoyée en date du 3 avril 2019 – dans son deuxième avis complémentaire, la Haute Corporation ne fit que deux observations relatives à l'annexe au PL 7314 ainsi que des observations d'ordre légistique –, les membres de la Commission de la Digitalisation, des Médias et des Communications adoptèrent dans leur réunion du 7 mai 2019 le présent projet de rapport relatif au dit projet de loi.

*

II. OBJET DU PROJET DE LOI

L'objet du projet de loi sous rubrique consiste en la transposition en droit national 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 (ci-après « la directive »).

Considérations générales

La digitalisation progressive de la quasi-totalité de notre société va de pair avec une croissance continue du nombre, de l'ampleur et des répercussions des attaques informatiques sur les systèmes et réseaux numériques. Dans notre ère numérique les systèmes d'information représentent dans beaucoup de cas des éléments essentiels pour le fonctionnement tant des entreprises que des administrations publiques, mais également en ce qui concerne la vie sociale des citoyens. Par conséquent il est inéluctable de renforcer constamment les efforts de sécurisation des systèmes et réseaux informatiques, d'autant plus que la connexion de toujours plus d'appareils électroniques augmente en parallèle la vulnérabilité et les sources de risque pour des attaques.

Partant, la directive vise à harmoniser et renforcer davantage la coopération des États membres en termes de gestion des risques cyber. Elle établit des règles communes horizontales pour ce qui est de la gestion de la sécurité cyber, en particulier en ce qui concerne les opérateurs qui fournissent des services essentiels, ainsi que les fournisseurs des services numériques. Les secteurs considérés essentiels au fonctionnement de la société sont les suivants : l'énergie, les transports, les banques, les infrastructures des marchés financiers, la santé, la fourniture et distribution d'eau potable et les infrastructures numériques. Ainsi les acteurs concernés doivent se soumettre à certaines obligations, à savoir, entre autres, à l'obligation de prendre toutes les précautions nécessaires pour assurer au mieux la sécurité de leurs systèmes informatiques, ou encore l'obligation de signaler les incidents qui ont un impact considérable sur leurs activités aux autorités compétentes. Le projet de loi prévoit notamment des critères détaillés pour déterminer la gravité d'un incident numérique.

Au niveau national, la directive prévoit le renforcement des capacités nationales. Les États membres doivent désigner des autorités nationales compétentes qui contrôlent le respect par les opérateurs de services essentiels et les fournisseurs de services numériques de leurs obligations respectives. De plus ils sont tenus à se doter d'équipes nationales de réponse aux incidents informatiques et d'élaborer une stratégie nationale de cybersécurité.

Finalement, au niveau européen, la coopération et l'échange d'informations sont renforcés. À cette fin, un groupe de coopération et un réseau de centres de réponse aux incidents de sécurité informatiques (« réseau des CSIRT (Computer Security Incident Response Teams) ») sont mis en place. Plus particulièrement, le rôle du groupe de coopération consiste à échanger des informations, du savoir-faire et de bonnes pratiques, ainsi que à encourager la coopération stratégique entre les États membres. Le réseau des CSIRT, quant à lui, sert à promouvoir une coopération opérationnelle rapide et effective entre les États membres.

*

III. AVIS DU CONSEIL D'ETAT

Avis du Conseil d'Etat du 10 juillet 2018

Le Conseil d'État a émis son premier avis en date du 10 juillet 2018. Le Conseil d'État estime qu'à bon nombre d'endroits les auteurs du projet de loi ont procédé à une transposition soit incorrecte, soit incomplète de la directive, ce qui oblige, par conséquent, la Haute Corporation à s'opposer formellement à l'égard de six articles du projet de loi sous avis. Ainsi les auteurs du présent projet de loi ont par exemple omis l'expression « *en particulier* » dans la phrase introductive de la liste qui définit les paramètres utilisés pour déterminer l'ampleur de l'impact d'un incident. L'effet de ceci consiste à transformer une liste de critères, à l'origine indicative et exemplative, en une liste limitative et exhaustive. De plus, le Conseil d'État demande qu'un nouvel article soit introduit pour transposer les dispositions de la directive relatives au pouvoir des autorités compétentes et du point de contact national unique de consulter les services répressifs nationaux compétents et les autorités nationales chargées de la protection des données, ainsi qu'à la collaboration de ces services et autorités, tel que prévu par l'article 8, paragraphe 6 de la directive.

Par ailleurs, si l'article 11 du projet de loi sous rubrique crée la base légale pour les autorités compétentes concernées d'imposer un certain nombre de contraintes aux fournisseurs de service numérique, il n'inclut toutefois pas la précision que les autorités compétentes se prêtent mutuellement assistance si nécessaire, comme le prévoit la directive. Il s'en suit alors que la Haute Corporation se voit obligée à s'y opposer formellement pour transposition incomplète de la directive.

Avis complémentaire du Conseil d'Etat du 27 novembre 2018

Le Conseil d'État a publié son avis complémentaire en date du 27 novembre 2018. Étant donné que les amendements introduits par les auteurs du présent projet de loi[3] tiennent compte des observations formulées par la Haute Corporation dans son premier avis, celle-ci est en mesure de lever l'intégralité de ses oppositions formelles.

Deuxième avis complémentaire du Conseil d'Etat du 26 avril 2019

Dans son avis du 26 avril 2019, le Conseil d'État marque son accord avec les amendements proposés[4].

*

IV. AVIS DES CHAMBRES PROFESSIONNELLES

Avis de la Chambre des métiers (29 août 2018)

Dans son avis du 29 août 2018, la Chambre des métiers n'a pas d'observations à formuler.

Avis de la Chambre de commerce (9 janvier 2018)

La Chambre de commerce a émis son avis en date du 14 novembre 2018. Dans celui-ci la Chambre de commerce renvoie à l'importance de transposer fidèlement la directive selon le principe « toute la directive, rien que la directive » afin de garantir que les entreprises luxembourgeoises ne se voient pas confrontées à des obligations plus strictes que celles valables pour les entreprises dans d'autres États membres. Ainsi elle regrette notamment que, selon le projet de loi sous rubrique, l'autorité compétente soit habilitée à porter un incident qui lui a été signalisé, à la connaissance du public dans plus de cas qu'il ne l'est prévu par la directive. Par ailleurs, en ce qui concerne le traitement de données person-

---

3 35 amendements gouvernementaux avaient été déposés en date du 2 octobre 2018.

4 Des amendements supplémentaires ont été adoptés par la Commission de la Digitalisation, des Médias et des Communications en date du 13 mars 2019 et en date du 3 avril 2019. L'objectif de ces amendements consiste principalement à tenir compte des observations d'ordre légistique formulées par le Conseil d'État dans son avis complémentaire du 27 novembre 2018, ainsi qu'à redresser certaines erreurs matérielles.

nelles, elle évoque également le risque de dédoublement des procédures entre celles introduites par le projet de loi et celles applicables en vertu du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et renvoie à la lourdeur administrative supplémentaire pour les acteurs concernés.

*

V. COMMENTAIRE DES ARTICLES

Article 1er

Le **paragraphe 1er de l'article 1er du PL 7314** détaille les entreprises et les prestataires de services de confiance auxquels les exigences en matière de sécurité et de notification prévues par le projet de loi ne s'appliquent pas.

Conformément à la directive « NIS» (Directive on security of network and information systems »), les obligations qui incombent aux

– opérateurs de services essentiels (OSE), et
– fournisseurs de service numérique (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.

Toutefois, si une telle 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 7 sont réunies.

Le **paragraphe 1er de l'article 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 **paragraphe 2 de l'article 1er du PL 7314** 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 oeuvre. Il est à noter que les Etats membres doivent fournir à la Commission des informations sur l'application de telles dispositions de lex specialis.

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.

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.

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) n° 1093/2010, et abrogeant la directive 2007/64/CE46 (« 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 ;

– 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 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 soumises à des obligations de sécurité pouvant être considérées comme équivalentes à celles énoncées par la directive NIS. 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.
– 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/UE52 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 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 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 11 de la loi NIS, qui pourraient être prises en considération dans l'application de l'article 1er, paragraphe 2, de la loi.

Article 2

L'article 2 du PL 7314 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 NIS »).

La définition sous **l'article 2, point 1, du PL 7314** 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 2 du PL 7314** définit l'opérateur de services essentiels (OSE), qui constitue, ensemble avec les fournisseurs de service numérique (FSN), l'un des acteurs principaux de la directive NIS.

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

Les FSN définis au **point 5 de l'article 2 du PL 7314** 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.

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 ».

Le **point 12 de l'article 2 du PL 7314** 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.

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.

Le « système de noms de domaine » (DNS), défini à **l'article 2, point 13, du PL 7314** 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.

Selon **l'article 2, point 15, du PL 7314**, 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.

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, 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.

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.

La place de marché en ligne, définie par le **point 16 de l'article 2 du PL 7314**, 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.

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. 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.

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.

Le moteur de recherche en ligne constitue le deuxième type de service numérique visé par la directive NIS (**article 2, point 17, du PL 7314**). 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. 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.

Le **point 18 de l'article 2 du PL 7314** 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.

- 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, 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.

Article 3

L'article 3 du PL 7314 constitue la réponse à une opposition formelle émise par le Conseil d'Etat à l'encontre de l'article 3 initial du projet de texte qui conférait un pouvoir réglementaire général aux autorités compétentes en matière de sécurité des réseaux et des systèmes d'information des différents secteurs énumérés à l'annexe du projet.

L'approche initialement choisie par les auteurs du projet de loi revenait à investir les autorités compétentes, à savoir la Commission de surveillance du secteur financier (CSSF) et l'Institut luxembourgeois de régulation (ILR) d'un pouvoir d'exécution similaire au pouvoir d'exécution dit « spontané » dont dispose le Grand-Duc au titre de l'article 36 de la Constitution. Or, le pouvoir réglementaire d'un établissement public ne saurait avoir la portée du pouvoir réglementaire du Grand-Duc, mais ne peut s'exercer qu'au titre d'une base légale précise qui en détermine les limites. Sous peine d'opposition formelle de la Haute Corporation, celle-ci avait dès lors demandé à ce que le texte du projet de loi soit complété avec les précisions nécessaires afin de limiter le pouvoir réglementaire des autorités compétentes concernées.

Figurant initialement au point 19 de l'ancien article 1er (article relatif aux définitions) du projet de texte, la désignation de la CSSF et de l'ILR en tant qu'autorités compétentes concernées est omise de cet article pour être rajoutée dans la partie normative du texte sous un nouvel article 3 remplaçant l'article 3 initial supprimé du texte.

En outre, la notion de « banque » a été remplacée par celle de « établissement de crédit », afin de refléter la nomenclature exacte du droit national et européen. Afin d'assurer une cohérence à travers le texte, le terme « banque » a également été remplacé dans le point 3 de l'annexe.

Au Luxembourg, la CSSF, ensemble avec l'ILR, 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 NIS 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, 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, indépendam-

ment 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.

Enfin, **l'alinéa 3 de l'article 3 du PL 7314** donne une autorisation expresse aux autorités compétentes d'échanger des informations et ce même si ces informations sont considérées confidentielles en vertu de l'article 16 de la loi modifiée du 23 décembre 1998 portant création d'une commission de surveillance du secteur financier et de 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'Etat. En effet, cette disposition permet à la loi de déroger au principe général du secret. Un tel échange d'informations entre autorités compétentes pourrait être de mise lorsqu'un même opérateur de services essentiels est susceptible de tomber dans le champ de compétence des deux autorités compétentes.

Article 4

Faisant suite aux recommandations du Conseil d'Etat et dans la lignée de la réflexion faite précédemment – le pouvoir réglementaire d'un établissement public ne saurait avoir la portée du pouvoir réglementaire du Grand-Duc, mais ne peut s'exercer qu'au titre d'une base légale précise qui en détermine les limites –, **l'article 4 du PL 7314** consiste à insérer dans la partie normative du projet de loi un texte qui figurait initialement dans l'article relatif aux définitions (point 20 de l'ancien article 1er).

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.

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 centres de réponse aux incidents de sécurité informatique (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. 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.

Article 5

L'article 5 du PL 7314 clarifie que l'intégralité des frais à charge de l'ILR et en relation avec la mise en place de la présente loi est couverte par une contribution financière étatique.

Article 6

L'ajout de **l'article 6** – dans son chapitre 2, dédié aux autorités compétentes concernées ainsi qu'au point de contact national unique, le projet de texte initial ne comprenait que trois articles – vise à répondre à une opposition formelle du Conseil d'Etat pour transposition incorrecte car incomplète de la directive « NIS ». En effet, le Conseil d'Etat demande la transposition de l'article 8, paragraphe 6 de ladite directive relative au pouvoir des autorités compétentes et du point de contact national unique de consulter les services répressifs nationaux et les autorités nationales chargées de la protection des données.

Afin de rendre cette coopération efficace, le secret auquel les agents de la CSSF sont tenus en vertu de l'article 16 de la loi modifiée du 23 décembre 1998 portant création d'une Commission de surveillance du secteur financier et les agents de l'ILR en vertu de 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'Etat ne s'applique pas au cas d'espèce.

Article 7

Le **paragraphe 1er de l'article 7 du PL 7314** précise que les OSE qui ont un établissement sur le territoire luxembourgeois tombent sous le champ d'application de la loi.

Dans son avis, le Conseil d'Etat avait recommandé d'insérer cette précision dans la partie des dispositions législatives normatives.

Par le fait que cette disposition figure en tant que disposition introductive au chapitre 3 relatif aux OSE, les auteurs du projet de texte ont voulu créer un parallélisme avec le chapitre 4 relatif aux FSN qui débute avec des précisions quant à son champ d'application.

Le **paragraphe 2 de l'article 7 du PL 7314** décrit le processus d'identification des OSE.

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 :

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 ;
   – 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 équivalentes à celles énoncées dans la loi NIS. 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 7, paragraphe 2, 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.

   Le nouveau **paragraphe 4 de l'article 7** propose de supprimer la disposition conférant un pouvoir réglementaire général aux autorités compétentes concernées et de compléter le projet de loi avec un nombre limité de cas dans lesquels les autorités compétentes disposent du pouvoir réglementaire. Ainsi, le **paragraphe 4** précise que la liste des services essentiels est fixée par l'autorité compétente concernée par voie de règlement.

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 7, paragraphe 2, point 2**).

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

   Ensuite, en vertu de **l'article 7, paragraphe 2, 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 7, paragraphe 3** :

- 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 ;
- 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 ;
- 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 ;
- 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 7, paragraphe 3**, pourraient inclure pour

- les fournisseurs d'énergie, le volume ou la proportion d'énergie produite au niveau national ;
- 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.

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 7, paragraphe 5**).

Article 8

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.

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. 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.

Dans son avis du 10 juillet 2018, le Conseil d'Etat relevait que le paragraphe 1er de l'article 7 du projet de texte initial manque de clarté en ce qu'il ne ressort pas du texte si l'autorité compétente concernée pourra déterminer un cadre d'analyse par voie règlementaire ou si l'autorité compétente devra adopter des décisions individuelles dans ce contexte. Vu l'insécurité juridique en découlant, le Conseil d'Etat s'était formellement opposé au texte. Il recommandait de

– soit exprimer le pouvoir réglementaire clairement dans le libellé de la disposition sous revue afin de garantir le respect de l'article 108*bis* de la Constitution,
– soit d'insérer cette précision à l'endroit de l'article 3 du texte initial.

En réponse à cette opposition formelle, les auteurs du projet de texte décidèrent alors de préciser le pouvoir réglementaire des autorités compétentes concernées dans différents articles. Ainsi, ce pouvoir réglementaire est ajouté à **l'article 8, paragraphes 1er, 3 et 5, alinéa 2**.

Bien que le **troisième paragraphe de l'article 8 du PL 7314** 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 outre un parallélisme avec la législation en matière de télécommunications qui exige une notification similaire à l'ILR.

Conformément à **l'article 8, paragraphe 4 du PL 7314**, 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 8, 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.

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, 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 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'Etat ne font 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 de l'article 8 du PL 7314** :

– le nombre d'utilisateurs touchés par la perturbation du service essentiel ;
– 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 ;
– la portée géographique eu égard à la zone touchée par l'incident.

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.

Par rapport au projet de texte initial, les termes « en particulier » sont rajoutés au **paragraphe 5 de l'article 8 du PL 7314** afin de répondre à une opposition formelle du Conseil d'Etat. En effet, la phrase introductive du **paragraphe 5** a, par dérogation à l'article 14, paragraphe 4, de la directive NIS, omis les termes « en particulier », transformant ainsi la liste indicative de paramètres utilisés pour mesurer l'ampleur de l'impact d'un incident en une liste limitative.

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 le point de contact luxembourgeois puisse assurer cette responsabilité, il faut qu'il dispose des informations nécessaires de la part des autorités compétentes (**paragraphe 7 de l'article 8 du PL 7314**).

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.

Finalement, le **paragraphe 8 de l'article 8 du PL 7314** 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 oeuvre 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.

Article 9

Afin de garantir que les autorités compétentes puissent contrôler et, le cas échéant, faire respecter les obligations énoncées dans la présente loi, **l'article 9 du PL 7314** 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 oeuvre effective des politiques de sécurité. Sur ce dernier point, **l'article 9, 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 oeuvre 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.

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.

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, le **paragraphe 3 de l'article 9 du PL 7314** 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.

Article 10

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.

Conformément au **paragraphe 2 de l'article 10 du PL 7314**, les FSN qui sont des microentreprises ou des petites entreprises au sens de la recommandation 2003/361/CE de la Commission du 6 mai 2003 concernant 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.

Article 11

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 cruciale 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.

Selon **l'article 10, paragraphe 1er, alinéa 2, du PL 7314**, 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.

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.

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.

Selon le **paragraphe 3 de l'article 11 du PL 7314**, 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, le **paragraphe 4 de l'article 11 du PL 7314** 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.

Le rajout des termes « en particulier » au **paragraphe 4 de l'article 11** (par rapport au paragraphe 4 de l'article 10 du projet de texte initial) vise à répondre à une opposition formelle formulée par le Conseil d'Etat. Comme soulevé à l'occasion du **paragraphe 5 de l'article 8 du PL 7314**, la Haute Corporation fait remarquer dans son avis du 10 juillet 2018 que les termes « en particulier » devraient être rajoutés dans le texte sous rubrique, afin de refléter l'esprit de la directive qui prévoit une liste exemplative de critères servant à mesurer l'importance de l'impact d'un incident.

Article 12

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 oeuvre les mesures prévues par **l'article 12 du PL 7314**, 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 12, paragraphe 1er**.

L'alinéa 1er du paragraphe 2 de l'article 12 du PL 7314 tient compte d'une opposition formelle formulée par le Conseil d'Etat. En effet, alors que la directive NIS prévoit que « 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 », la version initiale du texte envisageait que « l'autorité compétente concernée luxembourgeoise coopère avec l'autorité compétente de ces autres Etats membres », en omettant de préciser que les autorités compétentes se prêtent mutuellement assistance si nécessaire. Ainsi, le **paragraphe 2** est modifié de sorte qu'aussi bien la coopération que l'assistance mutuelle entre autorités compétentes concernées soient visées.

L'alinéa 2 du paragraphe 2 de l'article 12 du PL 7314 autorise les autorités compétentes luxembourgeoises et étrangère de coopérer, sans que le secret auquel les personnes exerçant une fonction au sein de la CSSF et celles exerçant une fonction au sein de l'ILR sont tenues en vertu de l'article 16 de la loi modifiée du 23 décembre 1998 portant création d'une commission de surveillance du secteur financier respectivement en vertu de 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'Etat ne saurait s'y opposer.

Article 13

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.

Article 14

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 8, 9, 11 et 12 du PL 7314** ou aux mesures prises en exécution de la loi NIS.

Remarquons que les sanctions administratives énumérées dans l'article 14 et la procédure y relative s'inspirent fortement de la législation existante dans les secteurs régulés par l'ILR. Le maximum des amendes d'ordre est fixé à 125.000 euros.

L'étendue du **paragraphe 5 de l'article 14 du PL 7314** se limite à l'ILR, puisque pour la CSSF, la question sera réglée par son règlement taxes.

Il est à noter que par rapport au projet de texte initial, **l'alinéa 3 du paragraphe 1er** est supprimé en ce qu'il se limite à répéter le principe que « les sanctions sont effectives, proportionnées et dissuasives ». En ce faisant, les auteurs des amendements se rallient à l'avis du Conseil d'Etat qui considère que cette disposition est dépourvue de toute valeur normative dans le cadre de la loi de transposition proprement dite.

Article 15

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 cryptographique, 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).

Article 16

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 oeuvre.

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 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 9*bis* 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.

Article 17

L'article 17 du PL 7314 détermine l'entrée en vigueur de la loi.

*

Compte tenu des observations qui précèdent, la Commission de la Digitalisation, des Médias et des Communications, propose, à l'unanimité de ses membres, à la Chambre des Députés d'adopter le projet de loi dans la teneur suivante :

*

TEXTE PROPOSE PAR LA COMMISSION DE LA DIGITALISATION, DES MEDIAS ET DES COMMUNICATIONS

7314

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 européenne et modifiant :

1° la loi modifiée du 20 avril 2009 portant création du Centre des technologies de l'information de l'Etat et

2° la loi du 23 juillet 2016 portant création d'un Haut-Commissariat à la Protection nationale

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 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 européenne ;

23° « 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 ;

24° « Point de contact national unique » : autorité qui 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 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'Etat 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'Etat 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'Etat 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 Etat membre, l'autorité compétente concernée consulte l'autorité compétente de l'autre Etat 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 Etats membres touchés si l'incident est susceptible d'avoir un impact significatif sur la continuité des services essentiels dans ces Etats 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 Etats 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) 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 oeuvre 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 oeuvre 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 Etats membres ou plus, l'autorité compétente concernée peut informer les autres Etats 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 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. 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 Etats membres, les autorités compétentes concernées luxembourgeoises et les autorités compétentes de ces autres Etats 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'Etat 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. 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, des domaines et de la TVA.

Chapitre 7 – *Dispositions modificatives*

Art. 15. A l'article 2, lettre y), de la 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. 16. La loi du 23 juillet 2016 portant création d'un Haut-Commissariat à la Protection nationale est modifiée comme suit :

1° A 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° A 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° A 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 oeuvre 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.

*

ANNEXE

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

Secteur	*Sous-secteur*	*Type d'entités*
	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. Etablissements de crédit		– 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 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

Secteur	*Sous-secteur*	*Type d'entités*
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 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

Impression: CTIE – Division Imprimés et Fournitures de bureau