N° 8364

CHAMBRE DES DEPUTES

PROJET DE LOI

concernant des mesures destinées à assurer un niveau élevé de cybersécurité et portant modification de :

1° la loi modifiée du 14 août 2000 relative au commerce électronique ;

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

3° la loi du 17 décembre 2021 sur les réseaux et les services de communications électroniques

***

Rapport de la Commission des Institutions

(13.04.2026)

La Commission se compose de : M. Laurent Zeimet, Président - rapporteur ; M. Guy Arendt, M. André Bauler, M. Gilles Baum, M. Marc Baum, Mme Simone Beissel, Mme Taina Bofferding, Mme Liz Braz, M. Mars Di Bartolomeo, M. Fred Keup, Mme Octavie Modert, Mme Nathalie Morgenthaler, Mme Sam Tanson, M. Charles Weiler, M. Michel Wolter, Membres.

* * *

SOMMAIRE

I.	**Antécédents**	**P. 2**
II.	**Objet**	**P. 2**
III.	**Considérations générales**	**P. 3**
IV.	**Avis**	**P. 5**
V.	**Commentaire des articles**	**P. 10**
VI.	**Texte proposé par la Commission**	**P. 38**

I. Antécédents

Le projet de loi sous rubrique a été déposé à la Chambre des Députés le 13 mars 2024 par M. Luc Frieden, Premier Ministre.

Au texte du projet de loi étaient joints un exposé des motifs, un commentaire des articles ainsi qu'une fiche financière, un *check* de durabilité et une fiche d'évaluation d'impact.

Le projet de loi a été renvoyé à la Commission des Institutions (ci-après la « Commission ») le 14 mars 2024.

Le 31 juillet 2024, la Chambre de Commerce a émis son avis.

Le 8 octobre 2024, le Conseil d'Etat a rendu son avis.

Le 9 décembre 2024, la Commission des Institutions a désigné M. Laurent Zeimet comme rapporteur du projet de loi. Lors de cette même réunion, elle a examiné le projet de loi ainsi que l'avis du Conseil d'Etat.

La Chambre des Métiers a émis son avis le 10 décembre 2024.

Le projet de loi a fait l'objet d'amendements gouvernementaux le 13 mai 2025.

Le 1er octobre 2025, la Chambre de Commerce a rendu un avis complémentaire.

Le Conseil d'Etat a émis son avis complémentaire le 8 décembre 2025.

Le Tribunal d'arrondissement de Luxembourg a rendu son avis le 22 décembre 2025.

Le 9 février 2026, la Commission a examiné les avis précités et a adopté une série d'amendements parlementaires.

Le 10 mars 2026, le Conseil d'Etat a émis son deuxième avis complémentaire.

Ledit avis a été examiné au cours de la réunion du 23 mars 2026.

Lors de sa réunion du 13 avril 2026 la Commission a adopté le présent rapport.

II. Objet

Le présent projet de loi a pour objet principal d'assurer la transposition en droit national de la directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) n° 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148, désignée ci-après comme directive NIS 2.

Cette directive remplace la directive (UE) 2016/1148 du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union, désignée ci-après comme directive NIS 1. Il vise ainsi à moderniser le cadre juridique national existant, notamment issu de la loi du 28 mai 2019 portant transposition de cette dernière.

La directive NIS 2 renforce le cadre européen en matière de cybersécurité en définissant des règles minimales communes, en améliorant la coopération entre États membres et en étendant le champ des secteurs soumis à des obligations en matière de cybersécurité, tout en prévoyant des mécanismes de supervision et d'exécution renforcés.

Dans ce contexte, le projet de loi a pour finalité de mettre en place un cadre national conforme aux exigences européennes, notamment en renforçant les obligations applicables aux entités concernées, en précisant le champ d'application du dispositif et en organisant les structures nationales compétentes en matière de cybersécurité.

Enfin, le projet de loi procède aux adaptations législatives nécessaires afin d'assurer la cohérence du droit national, notamment par l'abrogation des dispositions de fond de la loi du 28 mai 2019 et par la modification de la loi modifiée du 23 juillet 2016 portant création d'un Haut-Commissariat à la protection nationale ainsi que de la loi du 17 décembre 2021 sur les réseaux et les services de communications électroniques.

La directive NIS 2 est à transposer en droit national au plus tard le 17 octobre 2024. Les dispositions qu'elle prévoit sont applicables à partir du 18 octobre 2024.

III. Considérations générales

À l'instar de la directive (UE) 2022/2555, le projet de loi n° 8364 opère une distinction entre les entités essentielles et les entités importantes.

La catégorie des entités essentielles comprend, en principe, des grandes entreprises qui sont actives dans des secteurs hautement critiques, comme le secteur de l'énergie, du transport, du secteur bancaire, des infrastructures des marchés financiers, de la santé, de l'eau potable, des eaux usées, de l'infrastructure numérique, de la gestion des services TIC, de l'administration publique et de l'espace. Les secteurs hautement critiques sont énumérés dans l'annexe I.

Les entités importantes regroupent, de manière générale, d'une part, les entreprises de taille moyenne actives dans les secteurs hautement critiques visés à l'annexe I et, d'autre part, les grandes entreprises ainsi que les entreprises de taille moyenne exerçant leurs activités dans les autres secteurs critiques énumérés à l'annexe II.

Cette seconde catégorie couvre notamment les services postaux et d'expédition, la gestion des déchets, la fabrication, la production et la distribution de produits chimiques, ainsi que la production, la transformation et la distribution des denrées alimentaires. Elle inclut également plusieurs branches de la fabrication industrielle, parmi lesquelles la fabrication de dispositifs médicaux, la fabrication de produits informatiques, électroniques et optiques, la fabrication d'équipements électriques, la fabrication de machines et d'équipements ainsi que la fabrication d'autres matériels de transport. S'y ajoutent encore les fournisseurs numériques et le secteur de la recherche.

Le projet de loi retient ainsi une approche combinant la taille de l'entreprise et le niveau de criticité du secteur d'activité pour déterminer les entités importantes.

Cette classification connaît toutefois certaines exceptions. Certaines entités sont en effet qualifiées d'essentielles indépendamment de leur taille, notamment les entités critiques au sens du projet de loi n° 8307 portant transposition de la directive (UE) 2022/2557 relative à la résilience des entités critiques. Sont notamment visés les prestataires de services de confiance qualifiés, les registres de noms de domaine de premier niveau, les fournisseurs de services DNS, certains fournisseurs de réseaux publics de communications électroniques constitués en moyennes entreprises ainsi que des entités de l'administration publique.

Par ailleurs, certaines entités publiques actives dans les domaines de la défense et de la sécurité nationale ont été exclues du champ d'application de certaines dispositions du projet de loi. Cette exclusion se justifie par l'existence de régimes spécifiques applicables à ces domaines, notamment dans le cadre de l'Organisation du traité de l'Atlantique Nord (OTAN), ainsi que par la nécessité d'éviter des chevauchements normatifs et de préserver la confidentialité des opérations. Des considérations analogues s'appliquent aux activités relevant de la sécurité nationale, notamment afin de garantir la discrétion nécessaire au fonctionnement du Service de renseignement de l'État et de maintenir la confiance de ses partenaires internationaux.

La principale différence entre les entités classifiées comme essentielles respectivement comme importantes réside dans la rigueur du contrôle auquel elles sont soumises.

Le projet de loi désigne l'Institut luxembourgeois de régulation (ILR) et la Commission de surveillance du secteur financier (CSSF) comme autorités compétentes. L'ILR est compétent pour l'ensemble des secteurs, à l'exception du secteur bancaire et des infrastructures des marchés financiers. La CSSF est compétente pour ces secteurs dans la mesure où ils relèvent de sa surveillance. Dans la mesure où ces secteurs font déjà l'objet d'une réglementation stricte, ils sont relativement peu affectés par les nouvelles dispositions.

Le projet de loi prévoit que les autorités compétentes établissent une liste des entités essentielles et importantes. À cette fin, les entités susceptibles d'entrer dans le champ d'application communiquent aux autorités compétentes les informations nécessaires à leur identification, lesquelles confirment ensuite leur désignation. Ce mécanisme se distingue de celui instauré sous le régime de la directive NIS 1, dans lequel les autorités compétentes procédaient elles-mêmes à l'identification des opérateurs de services essentiels.

Parmi les innovations introduites figure le renforcement du rôle des organes de direction en matière de cybersécurité. Ceux-ci doivent approuver les mesures de gestion des risques, en superviser la mise en œuvre et peuvent être tenus pour responsables en cas de manquement. Ils sont en outre tenus de suivre régulièrement des formations et de veiller à la formation du personnel.

Les entités essentielles et importantes sont soumises à des obligations en matière de gestion des risques de cybersécurité, comprenant notamment l'analyse des risques, la sécurisation des systèmes d'information ainsi que la gestion des incidents et des crises. Une obligation de notification est prévue pour tout incident important.

En cas de violation des obligations prévues par la loi, ces entités s'exposent à des sanctions administratives, telles qu'un avertissement, un blâme ou une amende administrative, lesquelles doivent être effectives, proportionnées et dissuasives.

Pour les entités essentielles, le montant maximal des amendes administratives est fixé à 10 millions d'euros ou à 2 % du chiffre d'affaires annuel mondial total de l'entreprise. Pour les entités importantes, ce plafond est fixé à 7 millions d'euros ou à 1,4 % du chiffre d'affaires annuel mondial total.

Le projet de loi prévoit également la désignation d'un point de contact unique chargé d'assurer la coopération avec les autres États membres ainsi qu'avec la Commission européenne et l'Agence de l'Union européenne pour la cybersécurité. Cette fonction est confiée au Haut-Commissariat à la protection nationale (HCPN), qui exerce également les fonctions d'autorité de gestion des crises cyber et représente le Luxembourg au sein du réseau européen EU-CyCLONe.

En outre, le projet de loi organise les capacités nationales de réponse aux incidents de sécurité informatique. Le HCPN, dans sa fonction de GOVCERT.LU, est compétent pour les administrations et services de l'État, les établissements publics ainsi que les entités critiques au sens de la directive (UE) 2022/2557. Pour les autres entités, le « Computer Incident Response Center Luxembourg » (CIRCL), opéré par le groupement d'intérêt économique Luxembourg House of Cybersecurity, est compétent.

Le HCPN est également chargé de l'élaboration d'une nouvelle stratégie nationale en matière de cybersécurité, appelée à remplacer celle mise en place dans le cadre de la directive NIS 1.

Le projet de loi n° 8364 s'inscrit dans un cadre plus large et est étroitement lié au projet de loi n° 8307 portant transposition de la directive (UE) 2022/2557 relative à la résilience des entités critiques.

IV. Avis

1. Avis du Conseil d'Etat

a. Avis du 8 octobre 2024

Dans son avis du 8 octobre 2024, le Conseil d'État reconnaît l'utilité du projet de loi, qui vise à transposer la directive NIS 2 et à assurer un niveau élevé commun de cybersécurité, tout en formulant des réserves quant à la conformité du texte au droit de l'Union européenne et aux exigences constitutionnelles luxembourgeoises.

Il constate que le projet de loi n° 8364 renvoie à plusieurs directives européennes, notamment à la directive NIS 1, et rappelle que ces instruments n'ont pas d'effet direct en droit national, de sorte que les renvois doivent être remplacés par des références à la législation nationale de transposition.

La Haute Corporation émet plusieurs oppositions formelles pour transposition incorrecte de la directive. Elle souligne que les directives doivent être mises en œuvre de manière contraignante et que leur exécution doit répondre aux exigences de clarté et de certitude des situations juridiques.

D'abord, elle s'oppose formellement à l'alinéa 3 du paragraphe 7 de l'article 1er, qui confère à l'ILR et à la CSSF un pouvoir réglementaire leur permettant de déterminer les actes juridiques sectoriels de l'Union européenne ayant un effet au moins équivalent à la loi en projet. Elle estime que cette délégation revient à habiliter les autorités nationales à se prononcer sur les effets d'actes du droit de l'Union, ce qui risque d'entraver son application uniforme et de créer des divergences entre les régimes applicables aux différentes entités selon l'autorité compétente dont elles relèvent, en méconnaissance de l'exigence de sécurité juridique.

Ensuite, elle s'oppose formellement à l'article 8, relatif aux tâches des CSIRT, pour double transposition incorrecte de la directive. D'une part, les exigences de disponibilité, de confidentialité et de continuité de service figurant au paragraphe 1er de l'article 11 de la directive NIS 2 sont reléguées au seul commentaire des articles, alors qu'elles doivent figurer dans le texte même de la loi. D'autre part, le point 3° du paragraphe 1er de l'article sous revue subordonne l'assistance des CSIRT aux entités concernées à une « demande » de ces dernières, alors que la directive ne conditionne pas l'action des CSIRT à une telle initiative.

Elle s'oppose également formellement à l'article 16, paragraphe 3, qui mentionne la possibilité pour « l'État luxembourgeois » d'intenter une « action en justice » contre une entité n'ayant pas désigné de représentant dans l'Union européenne, sans préciser la juridiction compétente ni la procédure applicable. Cette imprécision contrevient aux exigences de clarté et de certitude des situations juridiques imposées par le droit de l'Union européenne, et méconnaît le principe de sécurité juridique consacré à valeur constitutionnelle par la Cour constitutionnelle.

Le Conseil d'État demande par ailleurs, sous peine d'opposition formelle, que l'article 18, paragraphe 6, soit complété en précisant l'objectif de la coopération imposée aux registres de noms de domaine de premier niveau et aux entités fournissant des services d'enregistrement, à savoir éviter toute répétition inutile dans la collecte des données d'enregistrement, conformément au texte de la directive.

Il s'oppose également formellement à l'article 22, paragraphe 4, point 9°, et à l'article 23, paragraphe 4, point 8°, qui se bornent à reproduire le libellé de la directive en renvoyant à des « organes compétents ou juridictions » dont l'identité n'est pas précisée dans le droit national, sans mettre en place le mécanisme que la directive exige de voir établi « conformément au droit national ». Il y voit une méconnaissance des exigences de spécificité, de précision et de clarté requises pour la transposition des directives, et une insécurité juridique quant à la nature des organes compétents pour infliger les amendes administratives prévues. Il demande à ce même titre, sous peine d'opposition formelle, que l'article 22, paragraphe 5, points 1° et 2°, soit reformulé de manière à garantir la spécificité, la précision et la clarté requises s'agissant des mesures de suspension et d'interdiction temporaire pouvant être prononcées à l'égard des entités essentielles défaillantes.

Enfin, le Conseil d'État s'oppose formellement aux paragraphes 4 et 5 de l'article 26 en raison d'une incohérence et d'un défaut de précision. Il constate que les comportements sanctionnables sont définis par un renvoi trop général aux articles 12 et 14, alors que les paragraphes 5 à 10 de l'article 14 ne comportent pas d'obligations sanctionnables. Il propose dès lors de limiter ce renvoi aux paragraphes 1er à 4 de l'article 14. En outre, la formulation relative aux amendes administratives, prévoyant un « montant maximal s'élevant à au moins […] », ne permet pas de déterminer avec précision le plafond des sanctions. Une telle détermination est pourtant nécessaire au respect du principe de légalité des peines garanti par l'article 19 de la Constitution.

Le Conseil d'État souligne par ailleurs l'étroite relation entre la directive NIS 2, que le projet de loi n° 8364 vise à transposer, et la directive (UE) 2022/2557 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience des entités critiques. Il rappelle qu'en vertu de

l'article 1er, paragraphe 2, de ladite directive, « les États membres veillent à ce que la présente directive et la directive (UE) 2022/2555 soient mises en œuvre de manière coordonnée », et préconise en conséquence que la loi transposant la directive (UE) 2022/2557 entre en vigueur au plus tard concomitamment avec la loi en projet.

Lors de sa réunion du 9 décembre 2024, la Commission des Institutions a décidé, à la lumière de cette observation, de traiter conjointement le projet de loi n° 8364 concernant des mesures destinées à assurer un niveau élevé de cybersécurité et le projet de loi n° 8307 portant transposition de la directive (UE) 2022/2557 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience des entités critiques.

b. <u>Avis complémentaire du 8 décembre 2025</u>

Dans son avis complémentaire du 8 décembre 2025, le Conseil d'État se penche sur les amendements gouvernementaux du 12 mai 2025 qui répondent en grande partie à ses observations formulées dans son avis du 8 octobre 2024. Il lève la plupart des oppositions formelles émises dans son premier avis.

Toutefois, la Haute Corporation maintient et émet plusieurs oppositions formelles.

D'abord, elle s'oppose formellement à l'article 1er, paragraphe 6, tel que modifié par l'amendement 9, qui exclut du champ d'application de la loi les entités exerçant dans les domaines de la « défense et de la sécurité nationale ». Elle estime que cette formulation est trop large et source d'insécurité juridique, et préconise de désigner nommément les autorités nationales concernées telles que le Service de renseignement de l'État ou l'Armée afin de garantir la précision requise par la directive.

Ensuite, elle s'oppose formellement à l'article 11, paragraphe 4, alinéa 3, tel que modifié par l'amendement 18, pour transposition incorrecte de la directive. Le texte offre en effet une simple « possibilité » aux autorités compétentes de mettre en place des mécanismes d'auto-enregistrement, alors que le législateur doit opérer un choix clair et contraignant pour assurer la certitude juridique exigée par le droit de l'Union européenne.

Une opposition formelle vise aussi l'article 16, paragraphe 3, tel que modifié par l'amendement 22, et l'article 22, paragraphe 5, tel que modifié par l'amendement 29. Ces dispositions omettent de désigner précisément la juridiction compétente, à savoir le président du Tribunal d'arrondissement de Luxembourg ou de Diekirch, pour statuer sur les actions en justice ou les mesures d'exécution à l'égard des entités n'ayant pas de siège au Grand-Duché de Luxembourg. La Haute Corporation insiste sur la nécessité de centraliser ces affaires devant une seule juridiction afin de satisfaire aux exigences de clarté et de sécurité juridique.

De façon générale, le Conseil d'État relève qu'aucune modification n'a été apportée à l'article 2, point 34°, et que la recommandation de remplacer « l'organisation judiciaire » par « les cours et tribunaux » n'a pas été suivie. Il rappelle que le terme « organisation judiciaire » est impropre, car il désigne l'ensemble des règles de fonctionnement des juridictions et non leurs organes. Il réitère dès lors sa demande de procéder à ce remplacement.

c. <u>Deuxième avis complémentaire du 10 mars 2026</u>

Dans son deuxième avis complémentaire du 10 mars 2026, le Conseil d'État examine les amendements parlementaires adoptés le 9 février 2026 et constate que ces modifications répondent de manière substantielle aux griefs formulés dans ses avis précédents, ce qui lui permet de lever l'intégralité des oppositions formelles qui subsistaient.

À la suite de la modification de l'article 11, paragraphe 4, alinéa 3, le Conseil d'État lève l'opposition formelle émise en raison d'une transposition incorrecte de la directive. Il lève également celle visant l'article 1er, paragraphe 6, les auteurs ayant désigné de manière expresse les autorités exclues du champ d'application de la loi, à savoir le Service de renseignement de l'État, la Direction de la défense et l'Armée luxembourgeoise. À cet égard, le Conseil d'État recommande toutefois de viser les « services du ministre ayant la Défense dans ses attributions » plutôt que la « Direction de la défense », cette dernière ne constituant qu'une subdivision ministérielle.

Enfin, les amendements désignant désormais précisément le président du Tribunal d'arrondissement de Luxembourg comme autorité compétente pour statuer sur les mesures d'exécution et les recours en matière de référé, les oppositions formelles relatives à l'insécurité juridique entachant les articles 16, paragraphe 3, et 22, paragraphe 5, sont également levées.

2. Avis de la Chambre de Commerce

a. Avis du 31 juillet 2024

Dans son avis du 31 juillet 2024, la Chambre de Commerce accueille favorablement le projet de loi, qu'elle salue pour son respect du principe de transposition fidèle de la directive NIS 2 selon l'adage « toute la directive, rien que la directive ». Elle indique pouvoir approuver le projet sous réserve de la prise en compte de ses remarques, portant principalement sur la sécurité juridique et la proportionnalité pour les opérateurs concernés.

S'agissant du champ d'application, la Chambre de Commerce s'interroge sur l'absence de précision quant aux délais d'enregistrement auprès des autorités compétentes et au délai de réponse de celles-ci pour confirmer la désignation en tant qu'entité essentielle ou importante.

Concernant les obligations substantielles, elle formule plusieurs observations et recommandations. Elle demande de limiter l'obligation relative à la chaîne d'approvisionnement prévue à l'article 12 aux seuls « principaux fournisseurs ou prestataires directs » et recommande de compléter l'article 13 afin que l'autorité compétente détermine par règlement le standard de formation applicable aux membres des organes de direction. Elle suggère également d'imposer une consultation publique préalable à l'adoption de tout règlement précisant les modalités de notification des incidents importants.

Sur le plan des mesures de supervision et des sanctions, la Chambre de Commerce recommande que les pouvoirs d'exécution prévus aux articles 22 et 23 soient listés par ordre croissant de gravité, de manière à garantir la proportionnalité des mesures prononcées. Elle regrette en outre que la fiche financière ne permette pas de percevoir clairement l'impact budgétaire global du projet de loi.

b. Avis complémentaire du 1er octobre 2025

Dans son avis complémentaire du 1er octobre 2025, la Chambre de Commerce se félicite de deux modifications introduites par les amendements gouvernementaux conformément à ses recommandations antérieures : l'amendement 17, qui prévoit un délai de deux mois à compter de l'entrée en vigueur de la loi pour la communication des informations d'enregistrement, et l'amendement 18, qui rend facultatif le recours aux mécanismes nationaux d'enregistrement tout en maintenant l'obligation de confirmation de la désignation en tant qu'entité essentielle ou importante.

Elle réitère néanmoins ses observations antérieures, portant sur la nécessité de préciser la portée des obligations relatives à la chaîne d'approvisionnement, de définir un standard de formation pour les membres des organes de direction et d'expliciter la gradation des sanctions afin d'en garantir la proportionnalité.

En ce qui concerne le champ d'application, la Chambre de Commerce formule trois nouvelles observations. Elle recommande d'intégrer expressément dans le dispositif normatif le critère d'indépendance d'une entité vis-à-vis de ses entreprises partenaires et liées aux fins de l'appréciation du critère de taille, relevant que ce critère, bien que mentionné dans le commentaire des articles, ne figure pas dans le texte de la loi. Elle suggère par ailleurs de limiter le champ d'application aux entités exerçant leur activité principale dans un secteur visé aux annexes I et II, et sollicite l'exclusion des entreprises de fabrication d'équipements électriques relevant du code NACE 27 lorsque ces activités sont exercées exclusivement à destination des particuliers.

3. Avis de la Chambre des Métiers du 10 décembre 2024

Dans son avis du 10 décembre 2024, rendu par voie d'autosaisine, la Chambre des Métiers se prononce en faveur d'un niveau élevé de sécurité des réseaux et des systèmes d'information et accueille favorablement le principe de transposition fidèle « toute la directive, rien que la directive ». Elle attire néanmoins l'attention sur la charge administrative et les investissements que l'élargissement du champ d'application est susceptible de générer pour les entreprises artisanales dépassant tout juste les seuils applicables aux petites entreprises.

En ce qui concerne le champ d'application, elle recommande d'exclure expressément les entreprises artisanales, dont la production sur mesure et en petites quantités ne présente pas l'importance cruciale pour le marché intérieur visée par le considérant 6 de la directive NIS 2. Elle suggère par ailleurs que les annexes I et II soient établies sur la base des activités visées par le droit d'établissement luxembourgeois plutôt que sur les codes NACE, et demande que la question de l'assujettissement des fournisseurs et prestataires des entités essentielles et importantes soit clarifiée.

Concernant les obligations substantielles et les sanctions, la Chambre des Métiers recommande aux autorités compétentes de publier des lignes directrices sectorielles et de privilégier une approche collaborative avant tout recours aux mesures coercitives. Elle sollicite un délai de mise en conformité prolongé pour les entreprises venant tout juste de franchir les seuils de la petite entreprise, ainsi que l'instauration d'une procédure obligatoire de mise en demeure préalablement à toute application d'amendes administratives.

La Chambre des Métiers indique ne pouvoir approuver le projet de loi que sous réserve de la prise en considération de l'ensemble de ces observations.

4. Avis du Tribunal d'arrondissement de Luxembourg du 22 décembre 2025

Dans son avis du 22 décembre 2025, le Tribunal d'arrondissement de Luxembourg se limite à se prononcer sur les amendements gouvernementaux n°s 22 et 29, qui sont les seuls à le concerner directement, les autres amendements n'appelant pas d'observation particulière de sa part.

S'agissant de l'amendement 22, le Tribunal accueille favorablement l'attribution d'une compétence au président du Tribunal d'arrondissement pour ordonner la désignation d'un représentant dans l'Union européenne. Il recommande toutefois de désigner expressément le président statuant comme juge unique, de retenir la formulation « statuant comme en matière de référé » plutôt que « siégeant comme juge des référés » afin d'éviter toute confusion avec les conditions restrictives de la procédure de référé, et de concentrer cette compétence devant une seule juridiction nationale afin de prévenir tout conflit de compétence entre les tribunaux de Luxembourg et de Diekirch.

S'agissant de l'amendement 29, le Tribunal formule des observations similaires quant à la terminologie applicable. Il recommande par ailleurs de supprimer la faculté offerte aux autorités compétentes de suspendre elles-mêmes une certification ou une autorisation, afin de confier cette compétence exclusivement au président du Tribunal d'arrondissement et de garantir ainsi les droits procéduraux des entités concernées. Il souligne enfin la nécessité de prévoir un mécanisme clair pour la cessation des mesures ordonnées par voie judiciaire, assurant à l'entité un contrôle juridictionnel effectif.

V. Commentaire des articles

Ad art. 1er

L'article 1er définit le champ d'application de la loi. D'abord, le paragraphe 1er fixe le principe que les micro et petites entreprises sont exclues du champ d'application de la loi sous projet. Ainsi, sont couvertes les entités publiques ou privées d'un secteur visé à l'annexe I ou II, qui constituent des entreprises moyennes[1] ou des grandes entreprises[2] en vertu de l'article 2 de l'annexe de la recommandation 2003/361/CE de la Commission des Communautés européennes du 6 mai 2003 concernant la définition des micro, petites et moyennes entreprises,[3] et qui fournissent leurs services ou exercent leurs activités au sein de l'Union européenne. Le champ d'application par secteur est étendu à une plus grande partie de l'économie pour assurer une couverture complète des secteurs et des services qui ont une importance cruciale pour les activités économiques et sociétales essentielles dans le marché intérieur.

Ensuite, le paragraphe 2 procède à une énumération limitative de cas dans lesquels le présent projet de loi sera entièrement applicable aux entités visées, peu importe leur taille. Ainsi, on retrouve parmi cette liste le cas de l'entité qui, au Luxembourg, est le seul prestataire d'un service essentiel au maintien d'activités sociétales ou économiques critiques, ou encore le cas de l'entité qui fournit un service dont la perturbation pourrait induire un risque systémique important.

Vu l'étroite relation entre la présente loi et la directive (UE) 2022/2557 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience des entités critiques, et abrogeant la directive 2008/114/CE du Conseil, ci-après « directive CER »,[4] il convient de veiller à ce que les champs d'application des deux textes s'articulent d'une manière cohérente.[5] Ainsi, selon le paragraphe 3,la loi s'applique à toutes les entités recensées en tant qu'entités critiques en vertu de ladite directive, quelle que soit leur taille.

---

[1] Une entreprise moyenne occupe au moins 50 personnes ou a un chiffre d'affaires annuel ou un total du bilan annuel d'au moins 10 millions d'euros, sans dépasser les seuils qui la qualifieraient de grande entreprise.

[2] Une grande entreprise est une entreprise qui occupe au moins 250 personnes ou dont le chiffre d'affaires annuel excède 50 millions d'euros ou dont le total du bilan annuel excède 43 millions d'euros.

[3] Recommandation 2003/361/CE de la Commission du 6 mai 2003 concernant la définition des micro, petites et moyennes entreprises, *J.O.U.E.*, L 124 du 20 mai 2003, p. 36.

[4] Directive (UE) 2022/2557 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience des entités critiques, et abrogeant la directive 2008/114/CE du Conseil, *J.O.U.E.*, L 333 du 27 décembre 2022, p. 164 ; projet de loi n° 8307 portant transposition de la directive (UE) 2022/2557 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience des entités critiques, et abrogeant la directive 2008/114/CE du Conseil, et modifiant : 1° la loi modifiée du 25 mars 2015 fixant le régime des traitements et les conditions et modalités d'avancement des fonctionnaires de l'État ; 2° la loi modifiée du 23 juillet 2016 portant création d'un Haut-Commissariat à la Protection nationale.

[5] Remarquons que, puisque la directive 2022/2557 est en cours de transposition (projet de loi n° 8307, cf. note 4), le texte de ce projet de loi fait référence à la directive elle-même.

Par analogie au projet de loi n° 8307 sur la résilience des entités critiques et portant modification de la loi modifiée du 23 juillet 2016 portant création d'un Haut-Commissariat à la Protection nationale, ci-après « projet de loi CER », la présente loi est aussi applicable aux administrations et entités qui exercent des activités dans le domaine de la sécurité nationale, de la sécurité publique, de la défense et de l'application de la loi, y compris la prévention et la détection des infractions pénales, ainsi que les poursuites en la matière. Alors que la directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) n° 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148, ci-après « directive NIS 2 »,[6] aurait permis de les exclure, les auteurs du projet de loi ont fait le choix de ne pas suivre cette voie, vu que déjà aujourd'hui certaines entités de ces secteurs ont été recensées comme critiques.

Le paragraphe 5 prévoit que la loi ne s'applique pas aux entités exclues du champ d'application du règlement (UE) 2022/2554 du Parlement européen et du Conseil[7] du champ d'application de la présente loi, conformément à l'article 2, paragraphe 4 dudit règlement.

Le paragraphe 6 exclut de l'application des articles 12, 13, 14 et 15 et du chapitre 6 du texte de loi le Service de renseignement de l'État, la Direction de la défense ainsi que l'Armée luxembourgeoise. La formulation s'inspire de la voie choisie par le législateur belge en désignant nommément les entités de l'administration publique visées par cette exclusion à l'instar de l'article 5, paragraphe 4, de la loi belge du 26 avril 2024 établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique.[8]
Il est rappelé que le secteur de la défense est d'ores et déjà soumis à une régulation distincte et spécialisée au niveau de l'Organisation du traité de l'Atlantique nord (OTAN). Imposer à ce secteur de devoir respecter en outre les exigences de la loi sous projet reviendrait à faire double emploi avec les obligations imposées par l'OTAN. De plus, soumettre le secteur de la défense à la loi sous projet reviendrait à lui imposer des obligations de rapportage additionnelles qui pourraient compromettre la confidentialité des opérations militaires et la confiance de ses partenaires internationaux.

En outre, l'article 1er, paragraphe 6, prévoit d'exclure le domaine de la sécurité nationale afin d'éviter de compromettre la confidentialité du travail du Service de renseignement de l'État, conformément à la loi modifiée du 5 juillet 2016 portant réorganisation du Service de renseignement de l'État, ainsi que la confiance de ses partenaires internationaux. Cette confiance constitue, en effet, une composante essentielle de la coopération internationale du Service de renseignement de l'État en vertu de l'article 9, paragraphe 4, de la loi précitée du 5 juillet 2016.

Le paragraphe 7 précise que la loi ne s'applique pas aux systèmes de communication et d'information où sont conservées ou traitées des pièces classifiées au sens de la loi précitée. D'une part, la loi du 15 juin 2004 prévoit que l'Autorité nationale de Sécurité (ANS) est l'autorité chargée de veiller à la sécurité des pièces classifiées et d'autre part, le projet de loi n° 6961 attribue à l'ANS certaines missions en relation avec les systèmes d'information classifiés.

[6] Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) n° 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148, *J.O.U.E.*, L 333 du 27 décembre 2022, p. 80.
[7] Règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) nº 1060/2009, (UE) nº 648/2012, (UE) nº 600/2014, (UE) nº 909/2014 et (UE) 2016/1011, *J.O.U.E.,* L 333, 27 décembre 2022, p. 1.
[8] *M.B.*, 17 mai 2024, p. 63179.

Ainsi, il reviendra notamment à l'ANS de définir une politique de sécurité en relation avec ces systèmes, de procéder à des inspections périodiques de ces systèmes et de participer à des groupes de travail ou des missions relatifs à la sécurité physique de lieux et de systèmes d'informations sensibles.[9] Afin de ne pas empiéter sur la compétence de l'ANS dans ce domaine, le présent projet de loi ne s'appliquera donc pas aux systèmes d'information classifiés.

Le paragraphe 8 prévoit que lorsque des dispositions d'actes juridiques sectoriels de l'Union européenne exigent des entités essentielles ou importantes qu'elles prennent des mesures de gestion des risques en matière de cybersécurité, ou notifient des incidents importants, et lorsque ces exigences ont un effet au moins équivalent aux obligations correspondantes prévues par la loi sous projet, les dispositions pertinentes du présent projet ne s'appliquent pas, de manière à éviter tout double emploi ou charge inutile. Dans un tel cas, les dispositions pertinentes de cet acte juridique sectoriel s'appliquent. Ainsi, le secteur de l'aviation dispose d'une réglementation qui impose à ses entités des obligations en matière de cybersécurité.[10] Notons que lorsqu'un acte juridique sectoriel de l'Union européenne ne couvre pas l'ensemble des entités d'un secteur visé dans la loi sous projet, les dispositions pertinentes de la présente loi s'appliquent pour ces entités.[11]

Ad art. 2

L'article 2 reprend la définition des termes employés dans la loi. Signalons que la grande majorité des définitions fait preuve d'une transposition fidèle de la directive NIS 2.

L'article 2, point 1°, définit la notion de « réseau et système d'information ». Cette définition vise à clarifier les types de systèmes et de réseaux qui sont couverts par le projet de loi, englobant à la fois les réseaux de communications électroniques tels que définis dans la loi du 17 décembre 2021 sur les réseaux et les services de communications électroniques[12] et les dispositifs interconnectés qui traitent des données numériques.

L'article 2, point 3°, définit le terme « cybersécurité ». La cybersécurité englobe toutes les actions nécessaires pour protéger les réseaux et systèmes d'information, les utilisateurs de ces systèmes et les autres personnes exposées aux cybermenaces.[13] Les cybermenaces représentent des risques pour la confidentialité, l'intégrité et la disponibilité des données, ainsi que pour la sécurité des utilisateurs finaux. En mettant l'accent sur la protection des utilisateurs et de toutes autres personnes exposées, le présent projet de loi adopte une

[9] Projet de loi n° 6961 portant 1. création de l'Autorité nationale de sécurité et 2. modification 1) de la loi modifiée du 15 juin 2004 relative à la classification des pièces et aux habilitations de sécurité ; 2) de la loi modifiée du 13 janvier 2019 instituant un Registre des bénéficiaires effectifs ; 3) du Code pénal, doc. parl. n° 6961[13].
[10] Consid. (29) directive NIS 2.
[11] Consid. (23) directive NIS 2.
[12] *Mém. A*, n° 927 du 22 décembre 2021. L'article 2, point 1, de cette loi se lit comme suit :
« « réseau de communications électroniques » : les systèmes de transmission, qu'ils soient ou non fondés sur une infrastructure permanente ou une capacité d'administration centralisée et, le cas échéant, les équipements de commutation ou de routage et les autres ressources, y compris les éléments de réseau qui ne sont pas actifs, qui permettent l'acheminement de signaux par câble, par la voie hertzienne, par moyen optique ou par d'autres moyens électromagnétiques, comprenant les réseaux satellitaires, les réseaux fixes (avec commutation de circuits ou de paquets, y compris l'internet) et mobiles, les systèmes utilisant le réseau électrique, pour autant qu'ils servent à la transmission de signaux, les réseaux utilisés pour la radiodiffusion sonore et télévisuelle et les réseaux câblés de télévision, quel que soit le type d'information transmise ; ».
[13] Article 2, point 1, règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) n° 526/2013, *J.O.U.E.,* L 151 du 7 juin 2019, p. 15.

approche holistique dans le but de minimiser les impacts négatifs des cybermenaces sur la société dans son ensemble.

Un incident, défini au point 5° de l'article 2, se réfère à un événement compromettant la disponibilité, l'authenticité, l'intégrité ou la confidentialité des données stockées, transmises ou faisant l'objet d'un traitement, ou des services que les réseaux et systèmes d'information offrent ou rendent accessibles. Les entités essentielles et importantes doivent être capables de prévenir les incidents les touchant ou susceptibles de les toucher. En outre, le projet de loi met en place un système de notification des incidents ayant un impact important sur la fourniture de leurs services.

La cybermenace est définie au point 9° du même article et constitue « *toute circonstance, tout événement ou toute action potentiels susceptibles de nuire ou de porter autrement atteinte aux réseaux et systèmes d'information, aux utilisateurs de tels systèmes et à d'autres personnes, ou encore de provoquer des interruptions de ces réseaux et systèmes* ».[14] Cette définition met en évidence la nature dynamique et en constante évolution des cybermenaces. En effet, les cybermenaces peuvent prendre de nombreuses formes, telles que des logiciels malveillants, des attaques de phishing, des violations de données, des dénis de service, ou autres.

Le point 17° explique le terme « point d'échange internet », qui est une structure de réseau qui permet l'interconnexion de plus de deux réseaux indépendants, également appelés systèmes autonomes. L'objectif principal de cette interconnexion est de permettre l'échange de trafic internet entre ces réseaux.

Ce point d'échange internet se distingue par deux caractéristiques essentielles. D'abord, il ne fournit une interconnexion que pour des systèmes autonomes, ce qui signifie qu'il est conçu spécifiquement pour faciliter la connectivité entre réseaux indépendants. Ensuite, il n'impose pas que le trafic internet échangé entre n'importe quelle paire de systèmes autonomes participant passe par un système autonome tiers, ni qu'il soit modifié ou altéré d'une manière quelconque.

Le « système de noms de domaine » (« DNS »), défini au point 18°, est un système hiérarchique et distribué qui attribue des noms aux services et aux ressources sur internet. L'attribution de noms permet l'identification desdits services et ressources, ce qui rend possible l'utilisation des services de routage et de connectivité internet par les dispositifs des utilisateurs finaux pour accéder à ces services et ressources. Le rôle principal du système est donc de traduire les noms de domaine assignés en adresses IP (*Internet Protocol*). 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.[15]

Vu qu'il est primordial de soutenir et de préserver un système de noms de domaine fiable, résilient et sécurisé afin de protéger l'intégrité de l'internet et d'assurer son fonctionnement continu et stable, la loi sous projet s'applique aussi aux fournisseurs de services DNS (point 19°) et aux registres de noms de domaine de premier niveau (point 20°).[16]

Le point 29°, définit le « service d'informatique en nuage ». Un service d'informatique en nuage est un service numérique qui permet l'administration à la demande et l'accès large à

[14] *Ibid.*, article 2, point 8.
[15] Annexe de la communication de la Commission au Parlement européen et au Conseil, « Exploiter tout le potentiel de la directive SRI – Vers la mise en œuvre effective de la directive (UE) 2016/1148 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union », C.O.M. (2017) 476 final, p. 25.
[16] Consid. (32) directive NIS 2.

distance à un ensemble, modulable et variable, de ressources informatiques, pouvant être partagées, même lorsque ces ressources sont réparties dans différents endroits. Les ressources informatiques comprennent des ressources telles que les réseaux, les serveurs ou d'autres infrastructures, les systèmes d'exploitation, les logiciels, le stockage, les applications et les services.[17]

- Les termes « administration à la demande » portent sur la capacité des utilisateurs de services d'informatique en nuage de se fournir eux-mêmes en capacités informatiques, comme du temps de serveur ou du stockage en réseau, sans aucune intervention humaine de la part du fournisseur.[18]

- Les termes « accès large à distance » portent sur le fait que les capacités en nuage sont fournies sur le réseau et que l'accès à celles-ci se fait par des mécanismes encourageant le recours à des plateformes clients légères ou lourdes disparates, y compris les téléphones mobiles, les tablettes, les ordinateurs portables et les postes de travail.[19]

- 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.[20]

- Le terme « variable » est utilisé pour décrire les ressources informatiques qui sont mises à disposition et libérées en fonction de la demande afin de pouvoir augmenter ou réduire rapidement les ressources disponibles en fonction de la charge de travail.[21]

- Les termes « pouvant être partagées » sont utilisées pour décrire les ressources informatiques 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.[22]

- Le terme « distribué » est utilisé pour décrire les ressources informatiques qui se trouvent sur des ordinateurs ou des appareils en réseau différents, qui communiquent et se coordonnent par transmission de messages.[23]

Le point 34° reprend la définition de l'entité de l'administration publique. Faute de définition de l'administration publique dans la législation luxembourgeoise, la référence au droit national a été omise dans le texte de transposition. En outre, alors que la directive NIS 2 exclut les entités de l'administration publique qui exercent leurs activités dans les domaines de la sécurité nationale, la sécurité publique, la défense ou de l'application de la loi, une telle exclusion n'est pas prévue par le projet de loi, de sorte que chaque entité qui répond aux critères de l'article 2, point 34°, est susceptible d'être considérée comme entité essentielle. Ainsi, le présent projet de loi se montre cohérent avec le projet de loi 8307[24] qui prévoit lui aussi que les entités des secteurs de la défense, de la sécurité publique et de la sécurité nationale peuvent être recensées comme entités critiques.

[17] Consid. (33) directive NIS 2.
[18] Consid. (33) directive NIS 2.
[19] Consid. (33) directive NIS 2.
[20] Consid. (33) directive NIS 2.
[21] Consid. (33) directive NIS 2.
[22] Consid. (33) directive NIS 2.
[23] Consid. (33) directive NIS 2.
[24] Projet de loi n° 8307, *o.c.*, (v. note 4).

Le point 40° précise la notion de « organisme de recherche », un nouveau type d'entité par rapport à la directive NIS 1.[25] Un organisme de recherche est une entité qui concentre l'essentiel de ses activités sur la conduite de la recherche appliquée ou du développement expérimental, en vue d'exploiter les résultats de recherche à des fins commerciales telles que la fabrication ou la mise au point d'un produit ou d'un processus, la fourniture d'un service ou la commercialisation d'un produit, d'un processus ou d'un service.[26]

Afin de faciliter la compréhension de la loi sous projet, la définition du « CIRCL » a été insérée au point 41°, et constitue dès lors, au niveau des définitions, un ajout par rapport au texte de la directive NIS 2. Le *Computer Incident Response Center Luxembourg* et le GOVCERT.LU constituent des centres de réponse aux incidents de sécurité informatique (CSIRT).

Finalement, les définitions des points 42°, 43° et 44° ont été ajoutées afin de préciser les dispositions sur la protection des données à caractère personnel (article 28 et suivants). En effet, les « données de communications électroniques », le « contenu de communications électroniques » et les « métadonnées de communications électroniques » constituent une partie des catégories de données qui sont susceptibles d'être traitées dans le contexte de ce projet de loi.

Ad art. 3

L'article 3 détermine les autorités compétentes chargées de veiller à l'application correcte du présent projet de loi.

D'une part, la loi sous projet s'insère dans la logique de la loi du 28 mai 2019 portant transposition de la directive NIS 1[27] et attribue à l'Institut Luxembourgeois de Régulation (ILR) la fonction d'autorité compétente en matière de sécurité des réseaux et des systèmes d'information pour la grande majorité des secteurs (énergie, transports, santé, eau potable, eaux usées, infrastructures numériques, services TIC, administration publique, espace, services postaux et d'expédition, gestion des déchets, fabrication, production, transformation et distribution de produits chimiques et de denrées alimentaires, fabrication, fournisseurs numériques, recherche).

D'autre part, vu l'expertise et la compétence de la Commission de surveillance du secteur financier (CSSF) en matière bancaire et financière, il a été jugé cohérent de lui confier le rôle d'autorité compétente pour le secteur bancaire et le secteur des infrastructures des marchés financiers. En outre, la CSSF est l'autorité compétente pour le secteur des infrastructures numériques et le secteur de la gestion des services TIC, en ce qui concerne les activités qui tombent sous la surveillance de la Commission de surveillance du secteur financier.

Afin d'assurer une bonne coopération entre les autorités compétentes et une approche cohérente en matière de cybersécurité, le troisième alinéa de l'article 3 prévoit une exception au secret professionnel inscrit dans les lois organiques respectives de la CSSF et de l'ILR,

[25] 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, *J.O.U.E.,* L 194 du 19 juillet 2016, p. 1.
[26] Consid. (36) directive NIS 2.
[27] Loi du 28 mai 2019 portant transposition de la directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union européenne et modifiant 1° la loi modifiée du 20 avril 2009 portant création du Centre des technologies de l'information de l'État et 2° la loi du 23 juillet 2016 portant création d'un Haut-Commissariat à la Protection nationale, *Mém. A* n° 372, 31 mai 2019, p. 1.

afin de permettre aux autorités compétentes, aux CSIRT et au point de contact unique d'échanger des informations en cas de besoin.

Ad art. 4

Alors que les nouvelles missions de la CSSF en tant qu'autorité compétente se recoupent largement avec le domaine de compétence actuel de la CSSF, l'ILR voit ses missions élargies notamment par le fait que le champ d'application de la directive NIS 2 englobe plus de secteurs que celui de la première directive NIS. De ce fait, l'ILR se voit accorder une contribution financière à charge du budget de l'État afin de couvrir l'intégralité des frais de fonctionnement qui résultent de l'exercice de ses missions prévues par la présente loi.

Ad art. 5

Afin d'assurer une cohérence entre la présente loi et le projet de loi CER,[28] le projet de loi accorde la mission d'ordre stratégique de point de contact unique au Haut-Commissariat à la Protection nationale (HCPN).

En tant que point de contact unique, le HCPN a pour mission de faciliter la coopération et la communication transfrontières et de permettre la mise en œuvre effective de la présente loi sous projet. Dans la mise en œuvre de cette mission, le point de contact unique est chargé de coordonner les tâches liées à la sécurité des réseaux et des systèmes d'information et de la coopération transfrontière au niveau de l'Union européenne.[29] Ainsi, le HCPN assure la coopération transfrontière des autorités compétentes luxembourgeoises avec les autorités compétentes des autres États membres, et, le cas échéant, avec la Commission et l'Agence de l'Union européenne pour la cybersécurité (ENISA), ainsi que la coopération intersectorielle avec les autres autorités compétentes nationales. La CSSF et l'ILR pourront également participer aux groupes de travail et de coopération ayant trait aux compétences respectives de ces autorités.

Ad art. 6

L'article 6 désigne le HCPN en tant qu'autorité compétente chargée de la gestion des incidents de cybersécurité majeurs et des crises, ci-après « autorité de gestion des crises cyber ». Le HCPN représente par ailleurs le Grand-Duché de Luxembourg au sein du réseau européen pour la préparation et la gestion des crises cyber, dénommé « EU-CyCLONe ».

Ad. art. 7

L'article 7 détermine les autorités compétentes pour la gestion des incidents de sécurité informatique qui pourraient menacer la stabilité et la sécurité des entités essentielles et importantes.

D'une part, le paragraphe 1er attribue au HCPN, dans sa fonction de GOVCERT.LU, la responsabilité de garantir la fonction de centre de réponse aux incidents de sécurité informatique (CSIRT) pour les administrations, les services de l'État, les établissements

[28] Projet de loi n° 8307, *o.c.*, (v. note 4).
[29] Consid. (39) directive NIS 2.

publics et les entités critiques en vertu de la directive CER. Ceci est en ligne avec les compétences que la loi modifiée du 23 juillet 2016[30] attribue au GOVCERT.LU.

D'autre part, la loi sous projet désigne le CIRCL en tant que CSIRT pour tous les autres cas, pour lesquels le HCPN, dans sa fonction de GOVCERT.LU, n'est pas compétent.

Le paragraphe 2 précise que les CSIRT couvrent les secteurs et sous-secteurs énumérés dans les annexes I et II du présent projet de loi, et qu'ils doivent suivre un processus bien défini pour la gestion des incidents. Les CSIRT doivent fournir une réponse rapide et adéquate pour faire face aux incidents de sécurité informatique.

Le paragraphe 3 souligne l'importance de la coopération entre les CSIRT et les communautés sectorielles ou intersectorielles d'entités essentielles et importantes. Cette coopération et l'échange d'informations sont essentiels pour anticiper et répondre efficacement aux menaces qui évoluent rapidement dans le domaine de la cybersécurité.

Ad art. 8

Le paragraphe 1er reprend le dispositif le paragraphe 1er de l'article 11 de la directive NIS 2, qui énonce les critères que les CSIRT doivent respecter pour garantir un niveau élevé de disponibilité, de confidentialité et de continuité de leur service.

Le paragraphe 2 liste les tâches des CSIRT. D'abord, les CSIRT ont une obligation générale de surveiller et d'analyser les cybermenaces et de diffuser des alertes. Les CSIRT veilleront à ce que les autorités compétentes soient informées de ces alertes. Ensuite, les entités essentielles et importantes peuvent demander l'assistance aux CSIRT pour la surveillance en temps réel ou quasi réel de leurs réseaux et systèmes d'information, pour la réaction aux incidents et pour la réalisation de scans proactifs de leurs réseaux afin de détecter des vulnérabilités éventuelles. En outre, les CSIRT jouent un rôle important dans les réseaux de coopération internationale, tels que le réseau des CSIRT. Vu que les cybermenaces peuvent entraîner des répercussions transfrontalières, le partage d'informations relève d'une importance primordiale. Enfin, dans la même lignée, le CIRCL est chargé de coordonner le processus de divulgation coordonnée des vulnérabilités en vertu de l'article 9, paragraphe 1er, de la présente loi sous projet, et les deux CSIRT contribuent au déploiement d'outils de partage d'informations sécurisés conformément à l'article 10, paragraphe 3, de la directive NIS 2.

Afin de pouvoir mener à bien leurs missions, les CSIRT respectent certaines exigences qui visent à garantir un niveau élevé de disponibilité, de confidentialité et de continuité de leur service, tels que :

- la disponibilité et communication : les CSIRT doivent maintenir un niveau élevé de disponibilité de leurs canaux de communication, en évitant les points de défaillance. Ils doivent disposer de plusieurs moyens de communication pour être contactés et pour contacter d'autres parties à tout moment. La spécification claire de ces canaux de communication est essentielle pour garantir une réponse rapide et efficace aux incidents ;

- la sécurité des locaux et des systèmes : les locaux des CSIRT, ainsi que les systèmes d'information qu'ils utilisent, doivent être situés sur des sites sécurisés ;

[30] Art. 3, para. 1*quater*, loi modifiée du 23 juillet 2016 portant création d'un Haut-Commissariat à la Protection nationale, *Mém*. A n°137 du 28 juillet 2016, p. 1.

- la gestion et le routage des demandes : les CSIRT doivent disposer d'un système de gestion et de routage des demandes approprié pour faciliter les transferts efficaces des informations et des demandes. Cela permet d'assurer une coordination efficace entre les différentes parties impliquées dans la gestion des incidents ;

- la confidentialité et fiabilité : les CSIRT sont tenus de garantir la confidentialité et la fiabilité de leurs opérations. Cela inclut la protection des données sensibles et la fourniture de services fiables pour les entités qui font appel à leurs services ;

- le personnel et la formation : les CSIRT doivent disposer du personnel adéquat pour assurer une disponibilité permanente de leurs services. De plus, ils doivent veiller à ce que leur personnel reçoive une formation appropriée pour faire face aux menaces et aux incidents ;

- la continuité de service : les CSIRT doivent être dotés des systèmes redondants et d'un espace de travail de secours pour garantir la continuité de leurs services, même en cas de perturbations majeures.

Le paragraphe 3 met l'accent sur l'importance de la coopération entre les CSIRT et le secteur privé. En effet, la collaboration et le partage d'informations entre les CSIRT et les acteurs du secteur privé permet de mieux anticiper les cybermenaces et de réagir plus efficacement aux incidents. Afin de faciliter cette coopération, les CSIRT encouragent l'adoption et l'utilisation de pratiques, de systèmes de classification et de taxonomies communs ou normalisés portant sur les procédures de gestion des incidents, la gestion de crise et la divulgation coordonnée des vulnérabilités en vertu de l'article 9, paragraphe 1er, du présent projet de loi.

Ad art. 9

L'article 9 porte sur la divulgation coordonnée des vulnérabilités qui se caractérise par un processus structuré dans lequel les vulnérabilités sont signalées au fabricant ou au fournisseur de produits TIC ou de services TIC afin qu'ils puissent diagnostiquer la vulnérabilité et y remédier.[31]

Le CIRCL, dans son rôle de coordinateur aux fins de la divulgation coordonnée des vulnérabilités, est un intermédiaire de confiance qui facilite les interactions entre la personne physique ou morale qui signale une vulnérabilité et le fabricant ou le fournisseur des produits TIC ou des services TIC potentiellement vulnérables.

Concrètement, le CIRCL est chargé d'identifier et de contacter les entités concernées et d'apporter une assistance aux personnes qui signalent une vulnérabilité. En sus, il négocie les délais de divulgation, gère les vulnérabilités qui touchent plusieurs entités (divulgation multipartite coordonnée de vulnérabilité) et coopère au sein du réseau du CSIRT, lorsque la vulnérabilité pourrait avoir un impact transfrontalier.[32]

Ce rôle d'intermédiaire est important pour faciliter le cadre volontaire de divulgation des vulnérabilités et pour garantir une communication fluide et la prise en compte rapide de la vulnérabilité signalée.

La possibilité est offerte aux personnes physiques ou morales de signaler une vulnérabilité de manière anonyme, si elles le souhaitent. Ceci favorise un environnement propice à la divulgation sans crainte de représailles et renforce la confiance des parties prenantes.

[31] Consid. (58) directive NIS 2.
[32] Consid. (61) directive NIS 2.

Une base de données européennes des vulnérabilités, mise en place par l'ENISA, permet l'accès en temps utile à des informations correctes relatives aux vulnérabilités touchant les produits et services TIC et contribue à une meilleure gestion des risques en matière de cybersécurité. Les entités, leurs fournisseurs de réseaux et de systèmes d'information, les autorités compétentes, ainsi que les CSIRT, peuvent, à titre volontaire, y divulguer et enregistrer les vulnérabilités publiquement connues afin de permettre aux utilisateurs de prendre les mesures d'atténuation appropriées.[33]

Ad art. 10

L'article 10 met en lumière l'importance de la coopération et de l'échange d'informations entre notamment les autorités compétentes, le point de contact unique et les CSIRT dans le cadre de la mise en œuvre de la loi sous projet.

Le paragraphe 2 souligne que les informations et les notifications concernant les incidents importants, les incidents, les cybermenaces et les incidents évités notifiées à l'autorité compétente doivent être transmises au CSIRT concerné et au point de contact unique. Cette transparence dans le partage d'informations est essentielle pour une réponse rapide et efficace aux incidents de cybersécurité.

Le paragraphe 3 de l'article 10 encourage la coopération entre les organes d'autres organismes, tels que les autorités répressives, les autorités chargées de la protection des données, les autorités nationales compétentes en matière de sûreté de l'aviation civile, les organes de contrôle en matière de transactions électroniques, les autorités de régulation des communications électroniques, et les autorités compétentes en vertu de la directive CER.

Vu que chaque entité critique en vertu de la directive CER constitue une entité essentielle et afin d'assurer la cohérence entre la mise en œuvre de la présente loi sous projet et de la directive CER, les autorités compétentes en vertu des deux textes coopèrent et échangent des informations sur le recensement des entités critiques, les risques, les cybermenaces et les incidents, sur les risques, menaces et incidents non cyber touchant les entités critiques, ainsi que sur les mesures prises pour faire face à ces risques, menaces et incidents.

Afin d'assurer une bonne coopération entre les autorités compétentes, le point de contact unique, les CSIRT, les autorités compétentes en vertu de la directive CER, et les autres organismes visés à l'article 10 du présent projet de loi, le paragraphe 5 prévoit une exception au secret professionnel inscrit dans les lois organiques respectives de la CSSF et de l'ILR.

Ad art. 11

L'article 11 décrit les entités qui relèvent du champ d'application du présent projet et qui sont donc soumises aux mesures de gestion des risques en matière de cybersécurité et aux obligations de notification. Les entités sont classées en deux catégories, entités essentielles et entités importantes, en fonction de la mesure dans laquelle elles sont critiques au regard du secteur ou du type de service qu'elles fournissent, ainsi que de leur taille.[34]

Les paragraphes 1er et 2 précisent les entités qui sont à considérer comme essentielles et importantes.

[33] Consid. (62) directive NIS 2.
[34] Consid. (15) directive NIS 2.

- En principe, les entités essentielles sont des grandes entreprises[35] actives dans des secteurs hautement critiques, spécifiés dans l'annexe I du projet de loi. Plus concrètement, il s'agit des secteurs de l'énergie (électricité, réseaux de chaleur et de froid, pétrole, gaz, hydrogène), du transport (transports aériens, transports ferroviaires, transports par eau, transports routiers), du secteur bancaire, des infrastructures des marchés financiers, de la santé, de l'eau potable, des eaux usées, de l'infrastructure numérique, de la gestion des services TIC, de l'administration publique et de l'espace.

- Les entités importantes sont en règle générale des moyennes entreprises[36] actives dans les secteurs hautement critiques de l'annexe I et les grandes entreprises ou moyennes entreprises actives dans les « autres secteurs critiques » spécifiés dans l'annexe II du projet de loi. Parmi les secteurs énumérés à l'annexe II figurent les services postaux et d'expédition, la gestion des déchets, la fabrication, la production et la distribution de produits chimiques, la production, la transformation et la distribution des denrées alimentaires, la fabrication (fabrication de dispositifs médicaux et de dispositifs médicaux de diagnostic in vitro, fabrication de produits informatiques, électroniques et optiques, fabrication d'équipements électriques, fabrication de machines et équipements n.c.a., construction de véhicules automobiles, remorques et semi-remorques, fabrication d'autres matériels de transport), les fournisseurs numériques et la recherche.

- Il existe néanmoins des exceptions à cette catégorisation. Ainsi, notamment les entités critiques en vertu de la directive (UE) 2022/2557[37] et les opérateurs de services essentiels identifiés sous la loi du 28 mai 2019 portant transposition de la directive NIS 1[38] sont tous considérés comme entités essentielles.

Remarquons que les entités essentielles sont soumises à des régimes de supervision et d'exécution plus stricts.[39]

Notons aussi que les considérants de la directive NIS 2 donnent des recommandations concernant les entreprises partenaires et les entreprises liées, afin d'éviter que celles-ci soient considérées comme entités essentielles ou importantes lorsque ceci serait disproportionné.[40] Ainsi, une évaluation au cas par cas devra déterminer le degré d'indépendance de l'entité en question par rapport à ses partenaires et entreprises liées en ce qui concerne le réseau et les systèmes d'information qu'elle utilise pour fournir ses services et en ce qui concerne les services qu'elle fournit. Par conséquent, le degré d'indépendance d'une entité pourra faire en sorte que celle-ci ne dépasse pas les seuils pertinents de la recommandation 2003/361/CE[41] et ne sera donc pas à considérer comme entité essentielle ou importante.

Le paragraphe 3 prévoit la création et la mise à jour régulière de listes des entités essentielles et importantes, ainsi que des entités fournissant des services d'enregistrement de noms de domaine par les autorités compétentes.[42] La régularité de la mise à jour garantit que les informations restent pertinentes et à jour. Ces listes devront par ailleurs être partagées au

[35] Une grande entreprise est une entreprise qui occupe au moins 250 personnes ou dont le chiffre d'affaires annuel excède 50 millions d'euros ou dont le total du bilan annuel excède 43 millions d'euros (art. 2 de l'annexe de la recommandation 2003/361/CE, *o.c.*, (v. note 3)).
[36] Une entreprise moyenne occupe au moins 50 personnes ou a un chiffre d'affaires annuel ou un total du bilan annuel d'au moins 10 millions d'euros, sans dépasser les seuils qui la qualifieraient de grande entreprise (art. 2 de l'annexe de la recommandation 2003/361/CE, *o.c.*, (v. note 3)).
[37] Projet de loi n° 8307, *o.c.*, (v. note 4).
[38] Loi du 28 mai 2019 portant transposition de la directive (UE) 2016/1148, *o.c.*, (v. note 27).
[39] Voir chapitre 6 du projet de loi.
[40] Consid. (16) directive NIS 2.
[41] Art. 2 de l'annexe de la recommandation 2003/361/CE, *o.c.*, (v. note 3).
[42] Consid. (18) directive NIS 2.

CSIRT compétent et au point de contact unique afin que ces derniers puissent remplir leurs missions respectives.

Enfin, le paragraphe 4 indique les informations que les entités concernées doivent au moins fournir aux autorités compétentes afin de compléter ces listes. Cela comprend des données de contact précises, des informations sur les secteurs et activités, sur leur présence géographique et sur leur taille et, le cas échéant, celle du groupe d'entités auquel l'entité appartient. Afin de faciliter la transmission de ces données, les autorités compétentes peuvent mettre en place des mécanismes nationaux permettant aux entités de s'enregistrer elles-mêmes.
Après que les entités se sont inscrites via le mécanisme national, l'autorité compétente leur confirme leur désignation en tant qu'entité essentielle ou importante.

Ad art. 12

Vu qu'il incombe aux entités essentielles et importantes de garantir la sécurité de leurs réseaux et systèmes d'information, l'article 12 impose à ces entités de mettre en place des mesures techniques, opérationnelles et organisationnelles appropriées et proportionnées pour gérer les risques qui menaceraient la sécurité de ces réseaux et systèmes et pour éliminer ou réduire les conséquences que les incidents auraient sur les utilisateurs de leurs services. Notons que ces entités devront garantir la sécurité de tous les réseaux et systèmes d'information qu'elles utilisent, indépendamment du fait que ces entités effectuent la maintenance de ces réseaux en interne ou qu'elles l'externalisent.[43]

Les mesures à mettre en place par les entités essentielles et importantes doivent englober des mesures visant à identifier tous les risques d'incidents, à prévenir et à détecter ces incidents, ainsi qu'à y réagir, à s'en rétablir, et à atténuer leurs effets. Elles doivent, d'une part, prendre en considération le degré de dépendance de l'entité essentielle ou importante à l'égard des réseaux et systèmes d'information.[44] D'autre part, elles devront répondre aux risques qui découlent de la chaîne d'approvisionnement d'une entité et de ses relations avec ses fournisseurs, tels que les fournisseurs de services de stockage et de traitement des données ou les fournisseurs de services de sécurité gérés et les éditeurs de logiciels.[45]

Les entités essentielles et importantes doivent, avant tout, mettre en place une variété de pratiques de cyberhygiène de base, notamment l'adoption de principes « confiance zéro », la mise à jour régulière des logiciels, la configuration des dispositifs, la segmentation des réseaux, la gestion des identités et des accès, ainsi que la sensibilisation des utilisateurs. De plus, ces entités doivent organiser des formations pour leur personnel et le sensibiliser aux cybermenaces. Elles doivent également évaluer leur propre niveau de préparation en matière de cybersécurité et, s'il y a lieu, poursuivre l'intégration de technologies de renforcement de la cybersécurité, telles que l'intelligence artificielle ou les systèmes d'apprentissage automatique, pour améliorer leurs capacités et renforcer la sécurité de leurs réseaux et systèmes d'information.[46]

A noter que les mesures à mettre en place ne devront pourtant pas être disproportionnées. Ainsi, les mesures devront être adaptées au niveau de risque existant, en prenant en considération l'état de l'art de ces mesures, les normes européennes et internationales applicables, ainsi que le coût de mise en œuvre.[47] La proportionnalité de ces mesures est

[43] Consid. (83) directive NIS 2.
[44] Consid. (78) directive NIS 2.
[45] Consid. (85) directive NIS 2.
[46] Consid. (89) directive NIS 2.
[47] Consid. (81) directive NIS 2.

évaluée en fonction de différents critères. Ainsi, il faudra prendre en compte la criticité de l'entité, les risques, y compris les risques sociétaux, auxquels elle est exposée, la taille de l'entité et la probabilité de survenance d'incidents et leur gravité.[48]

L'alinéa 3 du paragraphe 1er prévoit qu'un règlement ou une circulaire de l'autorité compétente précisera un cadre d'analyse des risques qui aidera les entités essentielles et importantes à identifier les risques. A l'instar de la transposition de la directive NIS 1, ce projet permet aux autorités compétentes de pouvoir demander aux entités essentielles et importantes d'utiliser un outil d'analyse de risque spécifique.

Les mesures de gestion des risques en matière de cybersécurité se fondent sur une approche « tous risques » (paragraphe 2). En d'autres mots, les mesures techniques, opérationnelles et organisationnelles doivent couvrir un large éventail d'éléments, notamment la gestion des incidents, la sécurité de la chaîne d'approvisionnement, la formation, la cybersécurité ou encore l'utilisation de solutions d'authentification à plusieurs facteurs.

Le paragraphe 2 est une ajoute par rapport à la directive. Ce paragraphe prévoit que les mesures mises en place par les entités essentielles doivent être notifiées à l'autorité compétente. Les modalités de cette notification seront précisées par l'autorité compétente par voie de règlement ou de circulaire. Cette précision est en ligne avec la transposition de la directive NIS 1[49] et constitue un parallélisme avec la législation en matière de télécommunications qui exige une notification similaire à l'ILR.[50]

Enfin, le paragraphe 5 insiste sur la nécessité pour les entités de prendre des mesures correctives en cas de non-conformité avec les mesures de gestion des risques en matière de cybersécurité.

Ad art. 13

L'article 13 souligne le rôle des organes de direction dans l'approbation des mesures de gestion des risques en matière de cybersécurité. Les membres des organes de direction ont la responsabilité de superviser la mise en œuvre de ces mesures et peuvent être tenus responsables en cas de violation de l'article 12.[51]

De plus, les membres des organes de direction et le personnel des entités essentielles et importantes sont tenus de suivre régulièrement une formation (paragraphe 2) et à offrir régulièrement une formation aux membres du personnel. Ces formations visent à ce que ces personnes aient les connaissances et les compétences nécessaires pour déterminer les risques et évaluer les pratiques de gestion des risques en matière de cybersécurité et leur impact sur les services fournis par l'entité. En favorisant la sensibilisation et la formation, les entités sont mieux préparées à faire face aux cybermenaces.

Ad art. 14

La procédure de notification et de gestion des incidents de cybersécurité est définie à l'article 14. Le texte de la directive tend à trouver un juste équilibre entre une notification rapide et efficace destinée à atténuer une propagation éventuelle, d'une part, et une notification

[48] Consid. (82) directive NIS 2.
[49] Art. 8, para. 3, loi du 28 mai 2019 portant transposition de la directive (UE) 2016/1148, *o.c.*, (v. note 27).
[50] Art. 42, para. 1er, al. 2, la loi du 17 décembre 2021 sur les réseaux et les services de communications électroniques, *Mém. A* n° 927, 22 décembre 2021.
[51] Consid. (137) directive NIS 2.

détaillée permettant une analyse approfondie des incidents qui augmentera la cyberrésilience des entités à moyen et long terme.[52]

D'abord, le paragraphe 1er dispose que les entités essentielles et importantes notifient à l'autorité compétente tout incident ayant un impact important sur leur fourniture de services (ci-après « incident important »). L'importance de l'incident est déterminée à l'aide d'une évaluation initiale effectuée par l'entité concernée et prend en compte, d'un côté, les perturbations opérationnelles graves des services de l'entité ou les pertes financières pour l'entité et, d'un autre côté, la nuisance à des personnes physiques ou morales en causant un dommage matériel, corporel ou moral considérable. Les considérants de la directive citent plusieurs exemples d'éléments jouant un rôle lors de cette évaluation initiale. Ainsi, l'entité concernée devra considérer les réseaux et les systèmes d'information touchés et notamment leur importance dans la fourniture des services de l'entité, la gravité et les caractéristiques techniques de l'incident, ainsi que l'expérience de l'entité en matière de traitement d'incidents similaires. Afin de déterminer la gravité de la perturbation opérationnelle du service, les entités devront tenir compte notamment de la mesure dans laquelle le fonctionnement du service est affecté, de la durée de l'incident et du nombre d'utilisateurs touchés.[53]

Lorsqu'une cybermenace importante est détectée, l'entité concernée en informe les destinataires de ses services afin de leur donner la possibilité de prendre des mesures pour se prémunir contre la menace ou pour atténuer ses effets (paragraphe 2). Alors que cette obligation d'information des destinataires devra être respectée dans toute la mesure du possible, elle ne saurait dispenser l'entité de prendre, de son côté, les mesures appropriées afin de prévenir et de gérer l'incident. Notons que la notification aux destinataires du service devra être gratuite et formulée dans un langage facilement compréhensible.[54]

Le paragraphe 4 établit le détail de la procédure de notification des incidents importants aux autorités compétentes. Ainsi, les entités concernées soumettent à l'autorité compétente, sans retard injustifié et au plus tard dans les vingt-quatre heures après avoir eu connaissance de l'incident, une notification préliminaire. Notons que les termes « alerte précoce » de la directive ont été remplacés par ceux de « notification préliminaire » afin d'éviter toute confusion avec le mécanisme d'alerte précoce activé par le CSIRT dans le cadre de l'article 8, paragraphe 1er. Remarquons que la notification préliminaire devra uniquement inclure les informations nécessaires pour porter l'incident important à la connaissance de l'autorité compétente et, le cas échéant, pour permettre à l'entité concernée de demander une assistance.[55]

La notification préliminaire est suivie, dans les soixante-douze heures après avoir eu connaissance de l'incident, d'une notification d'incident. Cette notification servira à mettre à jour les informations transmises lors de la notification préliminaire et fournira une évaluation initiale de l'incident.

Signalons que ni la notification préliminaire, ni la notification proprement dite ne devront détourner les ressources de l'entité concernée des activités liées à la gestion des incidents qui devraient avoir la priorité.

Après avoir reçu la notification préliminaire et la notification d'incident, l'autorité compétente ou le CSIRT peuvent demander à l'entité concernée de soumettre un rapport intermédiaire et, au plus tard un mois après la présentation de la notification d'incident, un rapport final.

[52] Consid. (101) directive NIS 2.
[53] Consid. (101) directive NIS 2.
[54] Consid. (103) directive NIS 2.
[55] Consid. (102) directive NIS 2.

Ensuite, l'autorité compétente, en coopération avec le CSIRT concerné, fournit une réponse à l'entité émettrice de la notification et, à sa demande, des orientations ou des conseils opérationnels sur la mise en œuvre d'éventuelles mesures d'atténuation (paragraphe 5).

Lorsqu'un incident important a un impact sur deux États membres ou plus, il est essentiel que le point de contact unique informe rapidement les États membres concernés ainsi que l'ENISA. Cette action vise à garantir une réponse coordonnée et efficace à l'incident, minimisant ainsi ses conséquences potentielles tout en garantissant les intérêts commerciaux des entités et la confidentialité des informations (paragraphe 6).

Lors de la survenance d'un incident important, il peut parfois être nécessaire de sensibiliser le public pour prévenir de futures menaces ou pour gérer la situation de manière appropriée. Lorsque la sécurité et les intérêts du public sont en jeu, l'autorité compétente, les CSIRT et les autorités compétentes des autres États membres peuvent, après avoir consulté l'entité concernée, informer le public de l'incident important ou exiger de l'entité qu'elle le fasse (paragraphe 7).

D'après le paragraphe 9, le point de contact unique soumet des rapports périodiques sur les incidents de cybersécurité à l'ENISA et, à la demande de l'autorité compétente, aux points de contact uniques des autres États membres touchés (paragraphe 8).

Enfin, le paragraphe 10 prévoit que les autorités compétentes, en vertu de la présente loi, fournissent aux autorités compétentes de la loi sur la résilience des entités critiques des informations sur les incidents importants, les incidents, les cybermenaces et les incidents évités notifiés.

Ad art. 15

Cet article permet à l'autorité compétente d'exiger des entités essentielles et importantes d'utiliser des produits, services et processus TIC spécifiques qui répondent aux normes de certification de cybersécurité européennes. Les prescriptions des autorités compétentes doivent être faites par voie de règlement et en prenant en considération les actes délégués adoptés par la Commission européenne Cette démarche vise à garantir la conformité aux exigences de l'article 12, renforçant ainsi la sécurité des entités essentielles et importantes, ainsi que celle des services essentiels qu'elles fournissent. L'utilisation de produits et services TIC certifiés permet de s'assurer que les technologies de l'information et des communications utilisées par ces entités répondent aux normes de sécurité les plus élevées, réduisant ainsi les risques liés à des cybermenaces.

Ad art. 16

L'article 16 traite de la compétence territoriale des autorités luxembourgeoises en définissant les cas dans lesquels une entité est considérée comme relevant de la compétence du Grand-Duché de Luxembourg.

Le paragraphe 1er énonce que les entités relevant du champ d'application de la présente loi sont soumises à la compétence du Grand-Duché de Luxembourg si elles y sont établies. Cependant, il y a des exceptions, notamment pour les fournisseurs de services de communications électroniques, les entités de l'administration publique et divers autres prestataires de services TIC. Ces entités sont soumises à la compétence de l'État membre

dans lequel elles fournissent leurs services, ont leur établissement principal dans l'Union européenne ou par lequel elles ont été établies.[56]

Le paragraphe 2 précise également comment déterminer l'établissement principal des fournisseurs de services DNS, des registres des noms de domaine de premier niveau, des entités fournissant des services d'enregistrement de noms de domaine, des fournisseurs de services d'informatique en nuage, des fournisseurs de services de centres de données, des fournisseurs de réseaux de diffusion de contenu, des fournisseurs de services gérés, des fournisseurs de services de sécurité gérés, ainsi que des fournisseurs de places de marché en ligne, de moteurs de recherche en ligne ou de plateformes de services de réseaux sociaux . Selon les considérants de la directive, l'établissement suppose l'exercice effectif d'une activité au moyen d'une installation stable. Cependant, la forme juridique de l'entité (filiale, succursale ou autre) ne joue aucun rôle à cet égard. En outre, la localisation physique du réseau et des systèmes d'information n'est pas déterminante afin d'identifier la localisation de l'établissement principal. Ce qui importe est de déterminer l'État membre dans lequel sont principalement prises les décisions relatives aux mesures de gestion des risques en matière de cybersécurité dans l'Union. Généralement, cet endroit est le lieu d'administration centrale des entités dans l'Union. S'il s'avérait impossible de déterminer dans quel État membre ces décisions étaient prises, il faudrait alors considérer que l'établissement principal se trouve dans l'État membre où sont effectuées les opérations de cybersécurité. Si, à nouveau, il n'est pas possible de déterminer cet État membre, il faudra considérer que l'établissement principal se trouve dans l'État membre où l'entité possède l'établissement comptant le plus grand nombre de salariés dans l'Union. Lorsque les services sont effectués par un groupe d'entreprises, il convient de considérer que l'établissement principal dans l'Union européenne qui exerce le contrôle est l'établissement principal du groupe d'entreprises au sens de la présente loi.[57]

Le paragraphe 3 concerne les entités citées ci-dessus non établies dans l'Union européenne qui offrent des services au Luxembourg. Afin de déterminer si une entité propose des services au Luxembourg, il convient d'examiner si elle envisage d'offrir des services à des personnes au Grand-Duché. Remarquons que la seule accessibilité du site Internet de l'entité ou d'un intermédiaire ou d'une adresse électronique ou d'autres coordonnées ou encore l'utilisation d'une langue généralement utilisée dans le pays tiers où l'entité est établie ne suffisent pas pour établir une telle intention. Cependant, des facteurs tels que la faculté d'acquérir des services en euros, l'utilisation d'une langue généralement utilisée au Luxembourg, avec la possibilité de commander des services dans cette langue ou la mention de clients ou d'utilisateurs qui se trouvent au Luxembourg pourraient indiquer que l'entité envisage d'offrir des services au Grand-Duché.[58]

Ces entités doivent désigner un représentant dans l'Union européenne, établi dans l'un des États membres où elles fournissent des services. Ce représentant devra agir pour le compte de l'entité et devra pouvoir être contacté par les autorités compétentes ou les CSIRT. Il devra être expressément désigné par un mandat écrit de l'entité le chargeant d'agir en son nom pour remplir les obligations, y compris la notification des incidents, qui lui incombent en vertu du présent projet.[59]
En l'absence d'un représentant dans l'Union européenne désigné en vertu du présent paragraphe et si l'entité fournit des services au Grand-Duché de Luxembourg, l'autorité compétente peut assigner l'entité à comparaître devant le président du tribunal d'arrondissement de Luxembourg statuant comme en matière de référé aux fins d'ordonner la désignation d'un représentant dans l'Union européenne.

[56] Consid. (113) directive NIS 2.
[57] Consid. (114) directive NIS 2.
[58] Consid. (116) directive NIS 2.
[59] Consid. (116) directive NIS 2.

Ad art. 17

L'article 17 traite de l'obligation des fournisseurs de services DNS, des registres de noms de domaine de premier niveau, des entités fournissant des services d'enregistrement de noms de domaine, des fournisseurs de services d'informatique en nuage, des fournisseurs de services de centres de données, des fournisseurs de réseaux de diffusion de contenu, des fournisseurs de services gérés, des fournisseurs de services de sécurité gérés, ainsi que des fournisseurs de places de marché en ligne, de moteurs de recherche en ligne ou de plateformes de services de réseaux sociaux de fournir certaines informations à l'autorité compétente.

D'après le paragraphe 1er, ces entités soumettent des informations spécifiques à l'autorité compétente, telles que le nom de l'entité, le secteur dans lequel elle opère, l'adresse de son établissement principal, ses coordonnées, les États membres dans lesquels elle fournit des services et ses plages d'IP. Ensuite, le point de contact unique transmet ces informations à l'ENISA pour la mise en place d'un registre, visé à l'article 27 de la directive NIS 2, afin d'assurer une bonne vue d'ensemble de ces entités.[60]

Ces entités doivent, en outre, notifier à l'autorité compétente toute modification des informations fournies dans un délai de trois mois à compter de la date de la modification (paragraphe 2).

Ad art. 18

L'article 18 concerne la collecte des données d'enregistrement des noms de domaine, en mettant l'accent sur la sécurité, la stabilité et la résilience du système de noms de domaine.[61]

Le paragraphe 1er dispose que les registres des noms de domaine de premier niveau et les entités fournissant des services d'enregistrement de noms de domaine sont tenus de collecter les données d'enregistrement avec diligence, conformément à la législation sur la protection des données personnelles, au sein d'une base de données spécialisée. Cette base de données contient des informations telles que le nom de domaine, la date d'enregistrement, les coordonnées du titulaire et du point de contact (paragraphe 2).

Afin de garantir la qualité des données relatives à l'enregistrement des noms de domaine, les registres des noms de domaine de premier niveau et les entités qui fournissent des services d'enregistrement de noms de domaine devront mettre en place des politiques et des procédures aux fins de collecter des données d'enregistrement de noms de domaine, de maintenir ces données exactes et complètes et pour prévenir et corriger les données d'enregistrement inexactes (paragraphe 3).[62]

En outre, le paragraphe 4 prévoit que les registres de noms de domaine de premier niveau et les entités d'enregistrement rendent publiques les données d'enregistrement qui ne sont pas des données personnelles, immédiatement après l'enregistrement du nom de domaine.[63]

Le paragraphe 5 concerne l'accès aux données d'enregistrement de noms de domaine par les demandeurs d'accès légitimes. Un demandeur d'accès légitime est une personne

[60] Consid. (117) directive NIS 2.
[61] Consid. (109) directive NIS 2.
[62] Consid. (111) directive NIS 2.
[63] Consid. (112) directive NIS 2.

physique ou morale qui formule une demande en vertu du droit de l'Union européenne ou du droit luxembourgeois, telle qu'une autorité compétente en vertu de la présente loi ou les autorités compétentes en matière de prévention et de détection d'infractions pénales, d'enquêtes et de poursuites. La demande d'accès doit être accompagnée d'une motivation permettant d'évaluer la nécessité d'accès aux données.[64] A cet effet, les registres des noms de domaine de premier niveau et les entités fournissant des services d'enregistrement de noms de domaine mettent en place des procédures d'accès qui pourraient notamment inclure l'utilisation d'une interface, d'un portail ou d'un autre outil technique afin de fournir un système efficace de demande et d'accès aux données d'enregistrement.[65] Les registres des noms de domaine de premier niveau et les entités fournissant des services d'enregistrement de noms de domaine sont tenus de répondre dans un délai de soixante-douze heures à ces demandes.

Enfin, le paragraphe 6 encourage la coopération entre les registres de noms de domaine de premier niveau et les entités d'enregistrement pour garantir la cohérence et l'efficacité de cette collecte de données. Il est important de veiller que la collecte des données d'enregistrement des noms de domaine n'entraine de répétition inutile.

Ad art. 19

L'article 19 de la loi sous projet met en lumière l'importance de la coopération et de l'échange d'informations en matière de cybersécurité pour les entités relevant de son champ d'application et celles ne relevant pas de son champ d'application. Dans un paysage numérique de plus en plus complexe et menaçant, le partage volontaire d'informations pertinentes sur les menaces et les vulnérabilités est essentiel et contribue à accroître la sensibilisation aux cybermenaces ainsi qu'à empêcher les menaces de se concrétiser.[66]

Le paragraphe 1er précise les objectifs de cet échange d'informations, notamment la prévention des incidents, la détection des menaces, la réaction à ces dernières, le rétablissement après incident et l'atténuation de leurs impacts. De plus, il souligne que cet échange d'informations doit contribuer à renforcer le niveau global de cybersécurité, en sensibilisant aux menaces, en limitant leur propagation, en remédiant aux vulnérabilités, et en mettant en œuvre des stratégies de défense et des techniques de détection et de prévention des menaces.

Le paragraphe 2 porte sur la mise en œuvre d'accords de partage d'informations en matière de cybersécurité pour faciliter l'échange d'informations. Ces accords doivent tenir compte de la nature sensible des informations. En outre, ces accords précisent les éléments opérationnels, y compris l'utilisation de plateformes TIC spécialisées et d'outils d'automatisation, le contenu et les conditions des accords de partage d'informations. Lorsque des autorités publiques participent à ces accords, des conditions en ce qui concerne les informations mises à disposition par les autorités compétentes ou les CSIRT peuvent être imposées. Les autorités offrent un soutien aux entités dans l'application de ces accords de partage d'informations.

Enfin, le paragraphe 3 souligne l'importance de notifier à l'autorité compétente la participation à de tels accords, ainsi que les retraits de ces accords.

Ad art. 20

[64] Consid. (110) directive NIS 2.
[65] Consid. (112) directive NIS 2.
[66] Consid. (119) directive NIS 2.

L'article 20 met en avant l'importance de la coopération volontaire et du partage d'informations en matière de cybersécurité. En effet, il établit un cadre qui permet aux entités essentielles et importantes, ainsi qu'à d'autres entités qui ne relèvent pas du champ d'application de la présente loi, de notifier à titre volontaire des incidents, des cybermenaces et des incidents évités aux autorités compétentes.

Le paragraphe 1er précise que ces notifications volontaires ne se substituent pas aux obligations de notification énoncées à l'article 14. Même si les entités essentielles et importantes sont tenues de notifier les incidents importants, elles sont encouragées à signaler d'autres incidents, menaces ou incidents évités de manière volontaire aux autorités compétentes. De même, les entités qui ne relèvent pas du champ d'application de la présente loi peuvent également contribuer à la sécurité des systèmes et réseaux d'information en signalant des incidents importants, des cybermenaces ou des incidents évités à l'Institut Luxembourgeois de Régulation. En effet, vu que la CSSF a une compétence très spécifique en matière bancaire et financière et que ces secteurs et les entités afférentes sont couverts par la présente loi, il a été jugé plus opportun de désigner l'ILR en tant qu'interlocuteur unique pour les entités qui ne relèvent pas du champ d'application du présent projet.

Le paragraphe 2 met en place un mécanisme de traitement des notifications volontaires par les autorités compétentes, en leur donnant la possibilité d'accorder la priorité aux notifications obligatoires afin que les incidents importants soient traités en premier lieu. De plus, il dispose que les informations pertinentes provenant de ces notifications volontaires peuvent être transmises au CSIRT concerné et au point de contact unique, tout en veillant à la confidentialité et à la protection appropriée des informations.

Enfin, l'article 20 souligne que, sans préjudice de la prévention et de la détection d'infractions pénales et des enquêtes et poursuites en la matière, le fait de signaler volontairement un incident n'entraîne pas d'obligations supplémentaires pour l'entité qui a effectué la notification. Cela vise, en effet, à encourager la divulgation proactive des incidents.

Ad art. 21

L'article 21 permet aux autorités compétentes de fixer des priorités en ce qui concerne les tâches de supervision selon une approche basée sur les risques. Cette approche permet aux autorités de hiérarchiser leurs actions de supervision et d'adapter leurs mesures en fonction des niveaux de risque associés aux différentes entités essentielles. Plus précisément, les autorités compétentes peuvent classer les entités essentielles en catégories de risque, en utilisant des critères et des valeurs de référence. En fonction de cette classification, elles peuvent recommander des mesures de supervision adaptées à chaque catégorie de risque. Cela peut inclure des méthodes telles que les inspections sur place, les audits de sécurité ciblés, les scans de sécurité, la collecte d'informations spécifiques, et le niveau de détail requis dans les rapports.[67]

Le paragraphe 2 souligne l'importance de la coopération entre les autorités compétentes en matière de cybersécurité et les autorités de contrôle 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 abrogeant la directive 95/46/CE. Cette coopération revêt une importance cruciale pour traiter les incidents liés aux violations de données à caractère personnel, garantissant ainsi une approche cohérente et coordonnée de ces questions.

[67] Consid. (124) directive NIS 2.

Ad art. 22

L'article 22 détaille les mesures de supervision et d'exécution que les autorités compétentes prennent à l'égard des entités essentielles. Les entités essentielles sont soumises à un régime de supervision à part entière, *ex ante* et *ex post*.[68] Ces mesures visent à garantir que ces entités respectent les obligations prévues par le présent projet et sont effectives, proportionnées et dissuasives compte tenu des circonstances spécifiques de chaque cas.

D'une part, parmi les pouvoirs de supervision accordés aux autorités compétentes, nous retrouvons (paragraphe 2) :

- les inspections sur place et les contrôles à distance ;
- les audits de sécurité ;
- les audits ad hoc ;
- les scans de sécurité ;
- les demandes d'informations ;
- les demandes d'accès à des données et documents ; et
- les demandes de preuves de mise en œuvre de politiques de cybersécurité.

Remarquons que lorsqu'un audit de sécurité est effectué par un organisme indépendant, les coûts en relation avec cet audit sont à la charge de l'entité contrôlée.

Les autorités compétentes s'assurent que les professionnels chargés de la supervision sont correctement formés et possèdent les compétences nécessaires pour mener à bien leurs missions. Cela inclut la capacité de réaliser des inspections sur place, ainsi que des contrôles hors site, tout en étant capables d'identifier les faiblesses potentielles dans les bases de données, le matériel, les pare-feux, le chiffrement et les réseaux.[69]

Il est important de noter que les mesures de supervision ne devront pas entraver inutilement les activités économiques des entités concernées. La nécessité de trouver un équilibre entre la sécurité numérique et la continuité des activités économiques est cruciale dans un environnement de plus en plus numérique. Alors que des mesures de supervision rigoureuses sont nécessaires pour garantir la sécurité des réseaux et des systèmes d'information, elles doivent être appliquées de manière à minimiser les conséquences économiques négatives.[70]

D'autre part, parmi les pouvoirs d'exécution accordés aux autorités compétentes figurent (paragraphe 4) :

- l'émission d'avertissements ;
- l'adoption d'instructions contraignantes ;
- l'ordonnance de mettre un terme à des comportements violant la loi ;
- l'ordonnance de mises en conformité spécifiques ;
- l'ordonnance d'informer les personnes susceptibles d'être affectées par une cybermenace ;
- l'ordonnance de mettre en œuvre les recommandations ;
- la désignation d'un responsable du contrôle du respect des articles 12 et 14 ;
- l'ordonnance de rendre publics les aspects de violations de la loi ; et
- l'imposition d'amendes administratives en vertu de l'article 24.

Lorsque les mesures ci-avant s'avèrent inefficaces, les autorités compétentes ont en outre le pouvoir de demander au président du Tribunal d'arrondissement de Luxembourg statuant

[68] Consid. (122) directive NIS 2.
[69] Consid. (125) directive NIS 2.
[70] Consid. (123) directive NIS 2.

comme en matière de référé de suspendre temporairement des certifications ou autorisations liées aux services fournis par l'entité ou d'interdire temporairement à des responsables dirigeants de l'entité d'exercer leurs fonctions (paragraphe 5). À noter que la suspension temporaire ne peut être infligée aux entités de l'administration publique relevant de la loi.

Le paragraphe 7 liste les circonstances que les autorités compétentes prennent en compte lors de la mise en œuvre des mesures d'exécution des paragraphes 4 et 5. Ainsi, sont notamment pris en compte la gravité de la violation, la durée de celle-ci, toute violation antérieure commise, les dommages causés, le fait que l'auteur de la violation a agi délibérément ou par négligence, les mesures prises par l'entité pour prévenir ou atténuer les dommages, l'application de codes de conduite, et la coopération des personnes responsables avec les autorités compétentes.

Selon le paragraphe 8, les autorités compétentes sont dans l'obligation d'exposer en détail les motifs de leurs mesures d'exécution aux entités essentielles et leur donnent un délai raisonnable afin de présenter leurs observations. Or, dans des situations dûment justifiées présentant une cybermenace importante ou un risque imminent, les autorités compétentes prennent des mesures d'exécution immédiates. Cela signifie qu'elles mettent en place des actions rapidement pour contrer les menaces, minimiser les dommages potentiels et protéger les réseaux et systèmes d'information.[71]

Enfin, les autorités compétentes collaborent avec d'autres autorités compétentes nationales, notamment dans le domaine de la résilience des entités critiques et de la résilience opérationnelle numérique du secteur financier, pour s'assurer du respect de la loi sous projet par les entités concernées (paragraphes 9 et 10).

Ad art. 23

L'article 23 traite des mesures de supervision et d'exécution applicables aux entités importantes. Il met en avant l'importance de ces mesures pour garantir la conformité des entités importantes à la réglementation en vigueur, en particulier en ce qui concerne les articles 12 et 14. Les entités importantes sont soumises à un régime de supervision léger, uniquement *ex post*. Les entités importantes ne sont pas tenues de notifier systématiquement leur conformité aux exigences en matière de gestion des risques de cybersécurité.

Le paragraphe 1er dispose que les autorités compétentes prennent des mesures de contrôle *ex post* basées sur des éléments de preuve, des indications ou des informations indiquant une possible violation de la loi. Ces éléments peuvent être soumis par diverses sources, y compris d'autres autorités, des citoyens, les médias ou d'autres entités, ou peuvent résulter des activités menées par les autorités compétentes.[72] Ces mesures doivent être efficaces, proportionnées et dissuasives, adaptées à chaque cas spécifique.

D'une part, le paragraphe 4 énumère les pouvoirs de supervision des autorités compétentes lorsqu'elles supervisent les entités importantes, notamment :

- la possibilité de mener des inspections sur place et des contrôles à distance ;
- la réalisation d'audits de sécurité ciblés par un organisme indépendant ou l'autorité compétente ;
- la réalisation de scans de sécurité ;
- la demande d'informations et de preuves ; et
- la demande d'accès à des données et à des documents.

[71] Consid. (126) directive NIS 2.
[72] Consid. (122) directive NIS 2.

D'autre part, le paragraphe 4 énumère les pouvoirs d'exécution des autorités compétentes, notamment la possibilité de :

- émettre des avertissements ;
- adopter des instructions contraignantes ;
- ordonner de mettre un terme à des comportements violant laloi ;
- ordonner des mises en conformité spécifiques ;
- ordonner d'informer les personnes susceptibles d'être affectées par une cybermenace ;
- ordonner de mettre en œuvre les recommandations ;
- ordonner de rendre publics les aspects de violations de la loi ;
- imposer des amendes administratives en cas de non-conformité.

De même que pour les entités essentielles, les autorités compétentes prennent des mesures d'exécution immédiates dans des cas dûment motivés présentant une cybermenace importante ou un risque imminent.[73]

Le paragraphe 5 prévoit que les paragraphes 6, 7 et 8 de l'article 22 du projet s'appliquent également aux entités importantes. Ce paragraphe offre une continuité dans l'approche réglementaire en matière de cybersécurité, en s'assurant que toutes les entités importantes sont soumises à des mécanismes de surveillance similaires, bien que potentiellement moins intensifs.

Selon le paragraphe 6, les autorités compétentes collaborent avec les autorités compétentes relevant du règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) n° 1060/2009, (UE) n° 648/2012, (UE) n° 600/2014, (UE) n° 909/2014 et (UE) 2016/1011. Cette coopération vise à renforcer la supervision et l'exécution des règles en matière de cybersécurité.

Ad art. 24

Cet article porte sur la coordination entre les autorités compétentes en vertu de la présente loi sous projet et les autorités de contrôle en matière de protection des données à caractère personnel. Tout d'abord, le paragraphe 1er souligne l'obligation des autorités compétentes de notifier sans délai injustifié les autorités de contrôle compétentes 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 abrogeant la directive 95/46/CE (ci-après « RGPD »)[74] lorsqu'elles ont connaissance d'une violation de données à caractère personnel.

En outre, si les autorités de contrôle imposent une amende administrative en vertu de l'article 58 du RGPD pour une violation dudit règlement, les autorités compétentes n'imposent pas une amende administrative supplémentaire en vertu de la présente loi sous projet pour une violation résultant du même comportement. Cependant, les autorités compétentes conservent la possibilité d'imposer d'autres mesures d'exécution prévues aux articles 22 et 23 (paragraphe 2).

[73] Consid. (126) directive NIS 2.
[74] *J.O.U.E.*, L 119, 4 mai 2016, p. 1.

Enfin, le paragraphe 3 souligne la nécessité de coopération entre les autorités compétentes en vertu de la présente loi et les autorités de contrôle compétentes en vertu du RGPD, en particulier lorsque l'autorité de contrôle est établie dans un autre État membre.

Ad art. 25

L'article 25, paragraphe 1er, porte sur les sanctions en cas de non-respect des obligations prévues par l'article 11, paragraphe 4, ainsi que les articles 13, 15, 17et 18, , garantissant que les entités essentielles ou importantes se conforment à cette loi et aux normes de cybersécurité requises. 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 peut imposer aux entités essentielles ou importantes des avertissements, des blâmes ou des amendes administratives. Les amendes administratives peuvent s'avérer significatives, atteignant un maximum de 250 000 euros.

La procédure contradictoire mise en place, dans le deuxième et troisième paragraphe, permet de protéger les droits de la défense, garantissant que les entités essentielles et importantes disposent d'un droit de consultation, d'observation et de recours. Cela assure un traitement équitable et transparent pour toutes les entités concernées. De plus, la possibilité d'un recours en réformation devant le tribunal administratif, prévue au paragraphe 4, offre une voie supplémentaire pour contester les décisions prises.

Remarquons que le régime de sanctions instauré par le présent projet s'inspire fortement de celui instauré par le projet de loi n° 8307 pour les entités critiques.[75]

Ad art. 26

L'article 26 définit le cadre relatif aux amendes administratives pour les entités essentielles et importantes en cas de violation de la loi sous projet. Suivant le paragraphe 2, les amendes administratives peuvent être imposées en complément des mesures d'exécution visées aux articles 22 et 23.

À noter que selon les considérants de la directive NIS 2, lorsqu'une amende administrative est infligée à une entité essentielle ou importante qui est une entreprise, le terme « entreprise » doit être interprété conformément aux articles 101 et 102 du traité sur le fonctionnement de l'Union européenne.[76] Lorsqu'une amende administrative est imposée à une personne qui n'est pas une entreprise, les autorités compétentes doivent tenir compte du niveau général des revenus et de la situation économique de la personne concernée lors de la détermination du montant de l'amende.[77]

Lors de la décision d'imposer une amende administrative et d'en fixer le montant il est tenu compte de plusieurs critères, prévus à l'article 22, paragraphe 7, tels que la gravité de la violation, la durée de la violation, toute violation antérieure commise, les dommages causés, le fait que l'auteur de la violation a agi délibérément ou par négligence, les mesures prises pour prévenir les dommages, l'application de codes de conduite, et le degré de coopération avec les autorités compétentes (paragraphe 3). Cette approche individualisée garantit que les sanctions sont adaptées à la situation et ne sont ni excessives, ni inadéquates.

[75] Art. 19 du projet de loi n° 8307, *o.c.*, (v. note 4).
[76] Traité sur le fonctionnement de l'Union européenne, *J.O.U.E.*, C 202 du 7 juin 2016, p. 47.
[77] Consid. (130) directive NIS 2.

Les paragraphes 4 et 5 prévoient le montant maximal des amendes pour les entités essentielles et importantes, en cas de violation des articles 12 ou 14 de la loi sous projet. Pour les entités essentielles, les amendes s'élèvent à un montant maximal de 10.000.000 euros ou à au moins 2% du chiffre d'affaires annuel mondial total de l'exercice précédent. Pour les entités importantes, les amendes s'élèvent à un montant maximal de 7.000.000 euros ou à au moins 1,4% du chiffre d'affaires annuel mondial total de l'exercice précédent. C'est le montant le plus élevé qui devra être retenu par l'autorité compétente lors de l'imposition de l'amende. Ces montants assez élevés permettent, en effet, de renforcer la clarté du dispositif et montrent que la cybersécurité est un enjeu de premier plan pouvant avoir un impact financier significatif. Il est à noter que ces amendes sont prononcées dans le respect de la procédure prévue à l'article 25 pour l'imposition de sanctions en cas de violation des obligations prévues aux articles 11, 13, 15, 17 et 18 (paragraphe 6).

En outre, selon le paragraphe 7, les autorités compétentes ont la possibilité d'assortir leur décision d'amende administrative d'une astreinte en vue de contraindre les entités essentielles ou importantes à mettre fin aux violations de la loi sous projet. Le montant total de l'astreinte ne pourra pas excéder 25 000 euros, sans dépasser 1 250 euros par jour.

Ad art. 27

L'article 27 aborde la coopération entre les autorités compétentes des différents États membres. Il met en lumière l'importance de la coordination et de l'assistance mutuelle pour garantir une application cohérente et efficace de la loi sous projet dans un environnement où les entités opèrent souvent au-delà des frontières nationales.

L'article dispose, dans son paragraphe 1er, que cette coopération comprend les éléments suivants :

- les autorités compétentes, en vertu de la présente loi, doivent informer et consulter, par le biais du point de contact unique, les autorités compétentes des autres États membres concernés sur les mesures de supervision et d'exécution qu'elles prennent ;

- les autorités compétentes peuvent demander à une autorité compétente d'un autre État membre de prendre des mesures de supervision ou d'exécution ;

- lorsqu'une demande d'assistance motivée est reçue d'une autorité compétente d'un autre État membre, l'autorité compétente, en vertu de la loi sous projet, fournit une assistance mutuelle proportionnée à ses ressources.

L'alinéa 2 du paragraphe 1er énonce également les circonstances dans lesquelles une demande d'assistance peut être refusée, notamment lorsque l'autorité compétente n'est pas compétente pour fournir l'assistance demandée, lorsque l'assistance demandée n'est pas proportionnée aux tâches de supervision de l'autorité compétente, ou lorsque la demande concerne des informations ou des activités contraires aux intérêts essentiels de la sécurité nationale, de la sécurité publique ou de la défense.

Le paragraphe 2 prévoit la possibilité pour les autorités compétentes en vertu de la présente loi et les autorités compétentes des autres États membres de mener des actions communes de supervision, d'un commun accord.

Ad. art. 28

L'article28 prévoit l'abrogation des lettres a) et b) du paragraphe 3 de l'article 45*bis* de la loi modifiée du 14 août 2000 relative au commerce électronique[78] sont abrogées.

La lettre a) porte sur les sanctions, visées à l'article 19, paragraphe 4, de la loi modifiée du 14 août 2000 relative au commerce électronique, en cas de non-respect du secret professionnel par toute personne chargée ou ayant été chargée de procéder à des audits auprès d'un prestataire de services de confiance. Afin d'assurer une bonne coopération entre les autorités compétentes, le point de contact unique et les CSIRT et en vue d'assurer une approche cohérente en matière de cybersécurité, les sanctions en cas de non-respect du secret professionnel sont abrogées. Ceci permet aux autorités de s'échanger des informations en cas de besoin.

La lettre b) porte sur les sanctions en cas de non-conformité aux exigences de notification d'incidents de sécurité visées à l'article 19, paragraphe 2, du règlement (UE) n° 910/2014.[79] Cet article est abrogé puisque les prestataires de services de confiance tombent entièrement sous le champ d'application de la présente loi et bénéficient ainsi du cadre juridique établi par ce projet. L'objectif est de rationaliser les obligations imposées auxdites entités en lien avec la sécurité des réseaux et systèmes d'information.[80]

Ad. art. 29

L'article 29 procède à des modifications de la loi-cadre du HCPN[81] afin d'y intégrer la nouvelle terminologie, d'une part, et de procéder à des adaptations ponctuelles devenues nécessaires, d'autre part.

D'abord, le point 1° de l'article 29 insère de nouvelles définitions dans la loi-cadre sous rubrique afin d'aligner la terminologie utilisée dans cette loi avec celle de la directive NIS 2.

Le point 2°, lettre a), remplace la notion de « stratégie nationale en matière de sécurité des réseaux et des systèmes d'information » par celle de « stratégie nationale en matière de cybersécurité », afin de tenir compte de la nouvelle terminologie introduite par la directive NIS 2.

Au point 2°, lettres b), d) et f), il est procédé à une modification organisationnelle au sein du HCPN. En effet, la lettre c) du paragraphe 1*bis* de l'article 3 est abrogée, de sorte à abolir le Service de la communication de crise. Alors que la communication de crise reste une mission que le HPCN assurera dans le cadre de la gestion de crise, il a été jugé plus logique, sur un plan purement organisationnel, d'intégrer le personnel du Service de la communication de crise dans le service du HCPN en charge de la prévention, de l'anticipation et de la gestion de crises. Afin que cette intégration réussisse complètement, il a été décidé de ne plus accorder de statut particulier au Service de la communication de crise.

Le point 2°, lettres c) et e), procèdent à des modifications concernant les dispositions en relation avec le GOVERT.LU.

D'abord, la dénomination de ce service (« CERT Gouvernemental ») est remplacée par celle de « GOVCERT.LU ». En effet, depuis sa création, le CERT Gouvernemental utilise

[78] Loi modifiée du 14 août 2000 relative au commerce électronique, *Mém.* A n°96 du 8 septembre 2000, p. 1.
[79] 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, *J.O.U.E.,* L 257 du 28 juillet 2014, p.73.
[80] Consid. (92) directive NIS 2.
[81] Loi modifiée du 23 juillet 2016, *o.c.*, (v. note 30).

l'acronyme GOVCERT(.LU) (*Government Computer Emergency Response Team*), un standard international utilisé dans le monde entier pour désigner les CSIRT gouvernementaux nationaux. Étant donné que le CERT gouvernemental est connu par ses partenaires nationaux et internationaux sous le nom GOVCERT.LU, il a été jugé opportun d'officialiser cette dénomination et de l'inscrire dans la loi.

Ensuite, la terminologie de l'article 3, paragraphe 1*quater* de la loi organique du HCPN est adaptée à celle utilisée dans la directive NIS 2. Ainsi, l'« incident de sécurité » est remplacé par celui d'« incident » et le « centre de traitement des urgences informatiques » est remplacé par le « centre de réponse aux incidents de sécurité informatique ».

En outre, alors qu'il y a des recoupements entre les lettres a) et b) dans la version actuelle du texte en ce que les deux points ont trait aux incidents, respectivement aux attaques informatiques, le texte modifié distingue clairement le rôle du traitement des incidents (lettre a)) et celui du service de veille, de détection, d'alerte et de réaction aux cybermenaces et aux vulnérabilités (lettre b)). De même, les termes de « cybermenace » et de « vulnérabilité », introduits par la directive NIS 2, se retrouvent dans les points subséquents concernant le CSIRT National et le MILCERT.LU.

Finalement, deux modifications sont faites en relation avec les entités critiques. Premièrement, il est dressé une distinction plus claire entre la mission du GOVCERT.LU et celle du CSIRT National. En effet, la prise en charge des entités critiques, qui tombait jusque lors sous la compétence du GOVCERT.LU, tombera dorénavant sous la compétence du CSIRT National. Puisque le CSIRT National est intégré dans l'équipe du GOVCERT.LU, cette modification n'aura aucun impact en pratique. Or, du point de vue logique, il est plus cohérent d'attribuer cette mission au CSIRT National et de limiter les compétences du GOVCERT.LU aux services étatiques. Notons que le GOVCERT.LU restera compétent pour les services étatiques qui se qualifient comme entité critique.

Deuxièmement, alors que le texte prévoit actuellement que le GOVCERT.LU assure, à la demande d'une entité critique (infrastructure critique), un service de réaction aux attaques informatiques et aux incidents de sécurité d'envergure, le texte modifié ajoute, d'une part, un service de veille aux cybermenaces et aux vulnérabilités et, d'autre part, précise que le CSIRT National apportera une assistance aux entités critiques. Cette deuxième modification résulte de la transposition de la directive NIS 2 qui prévoit que les CSIRT ont la tâche de « réagir aux incidents et apporter une assistance, à leur demande, aux entités essentielles et importantes concernées ».[82]

Ensuite, la loi remplace, en son point 3° et en ligne avec la nouvelle terminologie de la directive NIS 2, le chapitre 4*bis* sur la stratégie nationale en matière de sécurité des réseaux et des systèmes d'information par un nouveau chapitre « La stratégie nationale en matière de cybersécurité ».

Vu que le HCPN est l'autorité compétente pour adopter une stratégie en matière de sécurité des réseaux et des systèmes d'information sous la directive 2016/1148[83], il a été jugé cohérent de désigner le HCPN compétent pour élaborer la stratégie nationale en matière de cybersécurité.

[82] Voir article 8, paragraphe 1er, point 3.
[83] 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, *J.O.U.E.,* L 194 du 19 juillet 2016, p. 1.
Voir aussi : Loi du 28 mai 2019 portant transposition de la directive (UE) 2016/1148, *o.c.*, (v. note 27).

La stratégie nationale en matière de cybersécurité est un élément-clé de la loi. Elle vise à parvenir à un niveau élevé de cybersécurité et à le maintenir. La stratégie contient les objectifs stratégiques, les ressources nécessaires pour atteindre ces objectifs, ainsi que les mesures politiques et réglementaires appropriées.

Le premier paragraphe précise les éléments que la stratégie nationale en matière de cybersécurité doit comprendre. Cette stratégie comprend les objectifs et priorités en matière de cybersécurité, un cadre de gouvernance visant à atteindre les objectifs et priorités et précisant les rôles et responsabilités des parties prenantes concernées, une évaluation des risques, un inventaire des mesures de préparation, de réaction et de récupération après incident, une liste des différents acteurs et autorités concernés, ainsi qu'un plan pour sensibiliser les citoyens à la cybersécurité. Un élément important de la stratégie est le cadre d'action pour une coordination renforcée entre les autorités compétentes en vertu de la présente loi et les autorités compétentes en vertu de la directive CER. Afin d'assurer que ces autorités fonctionnent de manière complémentaire, la stratégie a pour objectif d'encourager le partage d'informations sur les risques, menaces et incidents cybernétiques et non-cybernétiques ainsi que d'inciter une collaboration au niveau de l'exercice des tâches de supervision.

Le paragraphe 2 constitue une nouveauté par rapport au texte de la directive NIS 1 et souligne les domaines spécifiques pour lesquels le HCPN devra élaborer des politiques dans le cadre de la stratégie nationale. Ces domaines comprennent par exemple l'élaboration de politiques de cyberhygiène. Ces politiques devront comporter une base commune de pratiques incluant notamment les mises à jour logicielles et matérielles, les changements de mots de passe, la gestion de nouvelles installations, la restriction de comptes d'accès de niveau administrateur et la sauvegarde de données.[84]

En outre, la lettre g) encourage la coopération avec les établissements universitaires et de recherche visant à faciliter l'utilisation de technologies innovantes, en particulier celles relatives aux outils automatisés ou semi-automatisés en matière de cybersécurité, et, s'il y a lieu, le partage des données nécessaires pour former les utilisateurs de ces technologies et les améliorer. En effet, ces technologies pourraient améliorer la détection et la prévention des cyberattaques.[85]

Le Luxembourg devra aussi élaborer une politique sur les partenariats public-privé afin d'offrir un cadre adapté aux échanges de connaissances, le partage de bonnes pratiques et l'établissement d'un niveau de compréhension commun à toutes les parties prenantes (lettre h)).[86]

Les politiques à élaborer dans le domaine de la cybersécurité devront aussi répondre aux besoins spécifiques des petites et moyennes entreprises (PME - lettre i)). En effet, alors que les PME représentent dans l'Union européenne une grande partie du marché de l'industrie et des entreprises, elles éprouvent souvent des difficultés à s'adapter aux nouvelles pratiques commerciales dans un monde plus connecté et à l'environnement numérique. Certaines de ces entreprises sont confrontées à des défis spécifiques en matière de cybersécurité - p.ex. une faible sensibilisation à la cybersécurité, un manque de sécurité informatique à distance, le coût élevé des solutions de cybersécurité et un niveau accru de menaces, comme les rançongiciels - pour lesquels elles devront recevoir des orientations et une assistance.Comme certaines PME ne gèrent pas les cyberrisques de manière adéquate, elles deviennent de plus en plus la cible d'attaques visant leur chaîne d'approvisionnement, qui ont souvent non

[84] Consid. (49) directive NIS 2.
[85] Consid. (51) directive NIS 2.
[86] Consid. (55) directive NIS 2.

seulement un impact sur leurs propres activités, mais peuvent aussi entraîner un effet en cascade sur les entreprises qu'elles approvisionnent.[87]

Finalement, les politiques nationales devront couvrir le volet de la promotion d'une cyberprotection active. Ainsi, au lieu de réagir aux cyberincidents, la cyberprotection active consiste en la prévention, la détection, la surveillance, l'analyse et l'atténuation actives des violations de la sécurité du réseau, combinées à l'utilisation de capacités déployées à l'intérieur et en dehors du réseau de la victime.[88]

Enfin, le nouvel article 9*bis* prévoit un mécanisme d'évaluation régulière de la stratégie nationale en matière de cybersécurité, au moins tous les cinq ans, garantissant ainsi son adaptation aux évolutions technologiques et aux menaces émergentes.

Le point 4°, ajoute, outre le chapitre 4*bis*, un nouveau chapitre 4*ter* à la loi-cadre du HCPN.

L'article 9*ter*, transposition fidèle de la directive NIS 2, prévoit que le HCPN est compétent pour adopter un plan national de réaction aux crises et incidents de cybersécurité majeurs. Cette approche va de pair avec la compétence du HCPN en tant qu'autorité de gestion des crises « tout risque ».

Selon le nouvel article 9*ter*, le plan national de réaction aux crises et incidents de cybersécurité majeurs contient plusieurs éléments, tels que les objectifs des mesures nationales de préparation, les tâches et les responsabilités du HCPN, en tant qu'autorité de gestion des crises cyber, les procédures de gestion des crises cyber, les mesures de préparation nationales, l'identification des parties prenantes et des infrastructures des secteurs public et privé concernées et les procédures et les arrangements nationaux entre les autorités et les organismes nationaux compétents en vue de garantir la participation et le soutien effectifs à la gestion coordonnée des incidents de cybersécurité majeurs au niveau de l'Union européenne.

Enfin, le point 5° de l'article 29, remplace les termes « Le personnel de l'ANSSI, du CERT Gouvernemental et du SCC » par ceux de « Le personnel de l'ANSSI et du GOVCERT.LU » afin de garder une cohérence avec l'abrogation du point 2°, lettre d) et de la nouvelle dénomination du Centre de réponse aux incidents de sécurité informatique.

Ad. art. 30

Sans commentaire.

Ad. art. 31

Les articles 42 et 43 de la loi du 17 décembre 2021 sur les réseaux et les services de communications électroniques[89] sont abrogés par l'article 31. Étant donné que les fournisseurs de réseaux de communications électroniques publics ou de services de communications électroniques accessibles au public tombent entièrement sous le champ d'application de la présente loi sous projet et bénéficient ainsi du cadre juridique établi par ladite loi, il y a lieu d'abroger l'article 42, portant sur les mesures de gestion des risques en matière de cybersécurité et l'obligation de notification des incidents, afin d'éviter toute

[87] Consid. (56) directive NIS 2.
[88] Consid. (57) directive NIS 2.
[89] Loi du 17 décembre 2021 sur les réseaux et les services de communications électroniques, *Mém*. A n° 927 du 22 décembre 2021, p. 1.

confusion ou incohérence. Pour les mêmes raisons, il y a lieu d'abroger l'article 43 qui porte sur la mise en œuvre et l'exécution, afin d'éviter tout double emploi. L'objectif est de rationaliser les obligations imposées auxdites entités en lien avec la sécurité des réseaux et systèmes d'information.[90]

Ad. art. 32

Finalement, l'article 32 introduit un intitulé de citation afin de faciliter la référence à la présente loi sous projet.

Annexes

Les annexes ont été reprises des annexes de la directive NIS 2 et font état des secteurs hautement critiques, d'une part, et des autres secteurs critiques, d'autre part.

VI. Texte proposé par la Commission

Sous le bénéfice des observations qui précèdent, la Commission des Institutions recommande à la Chambre des Députés d'adopter le projet de loi n°8364 dans la teneur qui suit :

Projet de loi

concernant des mesures destinées à assurer un niveau élevé de cybersécurité et portant modification de :

1° la loi modifiée du 14 août 2000 relative au commerce électronique ;

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

3° la loi du 17 décembre 2021 sur les réseaux et les services de communications électroniques

Chapitre 1er – Champ d'application et définitions

Art. 1er. (1) La présente loi s'applique aux entités publiques ou privées d'un type visé à l'annexe I ou II qui constituent des entreprises moyennes en vertu de l'article 2 de l'annexe de la recommandation 2003/361/CE de la Commission des Communautés européennes du 6 mai 2003 concernant la définition des micro, petites et moyennes entreprises, ou qui dépassent les plafonds prévus au paragraphe 1er dudit article, et qui fournissent leurs services ou exercent leurs activités au sein de l'Union européenne.

L'article 3, paragraphe 4, de l'annexe de ladite recommandation ne s'applique pas aux fins de la présente loi.

[90] Consid. (92) directive NIS 2.

(2) La présente loi s'applique également aux entités d'un type visé à l'annexe I ou II, quelle que soit leur taille, dans les cas suivants :

1° les services sont fournis par :

a) des fournisseurs de réseaux de communications électroniques publics ou de services de communications électroniques accessibles au public ;
b) des prestataires de services de confiance ;
c) des registres des noms de domaine de premier niveau et des fournisseurs de services de système de noms de domaine ;

2° l'entité est, au Grand-Duché de Luxembourg, le seul prestataire d'un service qui est essentiel au maintien d'activités sociétales ou économiques critiques ;

3° une perturbation du service fourni par l'entité pourrait avoir un impact important sur la sécurité publique, la sûreté publique ou la santé publique ;

4° une perturbation du service fourni par l'entité pourrait induire un risque systémique important, en particulier pour les secteurs où cette perturbation pourrait avoir un impact transfrontière ;

5° l'entité est critique en raison de son importance spécifique au niveau national ou régional pour le secteur ou le type de service en question, ou pour d'autres secteurs interdépendants au Grand-Duché de Luxembourg ;

6° l'entité est une entité de l'administration publique telle que définie à l'article 2, point 34°.

(3) La présente loi s'applique aux entités recensées en tant qu'entités critiques en vertu de la loi du XXX sur la résilience des entités critiques, quelle que soit leur taille.

(4) La présente loi s'applique aux entités fournissant des services d'enregistrement de noms de domaine, quelle que soit leur taille.

(5) La présente loi ne s'applique pas aux entités exclues du champ d'application du règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) n° 1060/2009, (UE) n° 648/2012, (UE) n° 600/2014, (UE) n° 909/2014 et (UE) 2016/1011 conformément à l'article 2, paragraphe 4, dudit règlement.

(6) Les articles 12, 13, 14 et 15 ainsi que le chapitre 6 ne s'appliquent pas :

1° au Service de renseignement de l'État visé par la loi modifiée du 5 juillet 2016 portant réorganisation du Service de renseignement de l'État ;
2° à la Direction de la Défense ;
3° à l'Armée luxembourgeoise visée par la loi modifiée du 7 août 2023 sur l'organisation de l'Armée luxembourgeoise.

Commenté [CC1]: les services du ministre ayant la Défense dans ses attributions cf. CE

Commenté [CC2R1]: A valider

(7) La présente loi ne s'applique pas aux systèmes de communication et d'information où sont conservées ou traitées des pièces classifiées au sens de la loi modifiée du 15 juin 2004 relative à la classification des pièces et aux habilitations de sécurité.

(8) Lorsque des actes juridiques sectoriels de l'Union européenne imposent à des entités essentielles ou importantes d'adopter des mesures de gestion des risques en matière de cybersécurité ou de notifier des incidents importants, et lorsque ces exigences ont un effet au moins équivalent à celui des obligations prévues par la présente loi, les dispositions

pertinentes de la présente loi, y compris celles relatives à la supervision et à l'exécution prévues au chapitre 6, ne sont pas applicables auxdites entités. Lorsqu'un acte juridique sectoriel de l'Union européenne ne couvre pas toutes les entités d'un secteur spécifique relevant du champ d'application de la présente loi, les dispositions pertinentes de la présente loi continuent de s'appliquer aux entités non couvertes par cet acte juridique sectoriel de l'Union européenne.

Les exigences visées à l'alinéa 1er du présent paragraphe sont considérées comme ayant un effet équivalent aux obligations prévues par la présente loi lorsque :

1° les mesures de gestion des risques en matière de cybersécurité ont un effet au moins équivalent à celui des mesures prévues à l'article 12, paragraphes 1er et 2 ; ou

2° l'acte juridique sectoriel de l'Union européenne prévoit un accès immédiat, s'il y a lieu, automatique et direct, aux notifications d'incidents par les CSIRT, les autorités compétentes ou les points de contact uniques en vertu de la présente loi, et lorsque les exigences relatives à la notification des incidents importants sont au moins équivalentes à celles prévues à l'article 14, paragraphes 1er à 6.

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, point 1°, de la loi du 17 décembre 2021 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 tout événement susceptible de compromettre la disponibilité, l'authenticité, l'intégrité ou la confidentialité de données stockées, transmises ou faisant l'objet d'un traitement, ou des services que ces réseaux et systèmes d'information offrent ou rendent accessibles ;

3° « cybersécurité » : la cybersécurité au sens de l'article 2, point 1°, du règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) n° 526/2013 (règlement sur la cybersécurité), tel que modifié ;

4° « incident évité » : un événement qui aurait pu compromettre la disponibilité, l'authenticité, l'intégrité ou la confidentialité des données stockées, transmises ou faisant l'objet d'un traitement, ou des services que les réseaux et systèmes d'information offrent ou rendent accessibles, mais dont la réalisation a pu être empêchée ou ne s'est pas produite ;

5° « incident » : un événement compromettant la disponibilité, l'authenticité, l'intégrité ou la confidentialité des données stockées, transmises ou faisant l'objet d'un traitement, ou des services que les réseaux et systèmes d'information offrent ou rendent accessibles ;

6° « incident de cybersécurité majeur » : un incident qui provoque des perturbations dépassant les capacités de réaction du seul État membre de l'Union européenne concerné ou qui a un impact important sur au moins deux États membres de l'Union européenne ;

7° « gestion des incidents » : toutes les actions et procédures visant à prévenir, détecter, analyser et contenir un incident ou à y répondre et à y remédier ;

8° « risque » : le potentiel de perte ou de perturbation causé par un incident, à exprimer comme la combinaison de l'ampleur de cette perte ou de cette perturbation et de la probabilité qu'un tel incident se produise ;

9° « cybermenace » : une cybermenace au sens de l'article 2, point 8°, du règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) n° 526/2013 (règlement sur la cybersécurité), tel que modifié ;

10° « cybermenace importante » : une cybermenace qui, compte tenu de ses caractéristiques techniques, peut être considérée comme susceptible d'avoir un impact grave sur les réseaux et les systèmes d'information d'une entité ou les utilisateurs des services de l'entité, en causant un dommage matériel, corporel ou moral considérable ;

11° « produit TIC » : un produit TIC au sens de l'article 2, point 12°, du règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) n° 526/2013 (règlement sur la cybersécurité), tel que modifié ;

12° « service TIC » : un service TIC au sens de l'article 2, point 13°, du règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) n° 526/2013 (règlement sur la cybersécurité), tel que modifié ;

13° « processus TIC » : un processus TIC au sens de l'article 2, point 14°, du règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) n° 526/2013 (règlement sur la cybersécurité), tel que modifié ;

14° « vulnérabilité » : une faiblesse, susceptibilité ou faille de produits TIC ou de services TIC qui peut être exploitée par une cybermenace ;

15° « 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, tel que modifié ;

16° « spécification technique » : 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, tel que modifié ;

17° « point d'échange internet » : une structure de réseau qui permet l'interconnexion de plus de deux réseaux indépendants (systèmes autonomes), essentiellement aux fins de faciliter l'échange de trafic internet, qui n'assure l'interconnexion que pour des systèmes autonomes et qui 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 ;

18° « système de noms de domaine » ou « DNS » : un système hiérarchique et distribué d'affectation de noms qui permet l'identification des services et des ressources internet, ce qui rend possible l'utilisation de services de routage et de connectivité internet par les dispositifs des utilisateurs finaux pour accéder à ces services et ressources ;

19° « fournisseur de services DNS » : une entité qui fournit :

a) des services de résolution de noms de domaine récursifs accessibles au public destinés aux utilisateurs finaux de l'internet ; ou
b) des services de résolution de noms de domaine faisant autorité pour une utilisation par des tiers, à l'exception des serveurs de noms de racines ;

20° « registre de noms de domaine de premier niveau » : une entité à laquelle un domaine de premier niveau spécifique a été délégué et qui est responsable de l'administration du domaine de premier niveau, y compris de l'enregistrement des noms de domaine relevant du domaine de premier niveau et du fonctionnement technique du domaine de premier niveau, notamment l'exploitation de ses serveurs de noms, la maintenance de ses bases de données et la distribution des fichiers de zone du domaine de premier niveau sur les serveurs de noms, que ces opérations soient effectuées par l'entité elle-même ou qu'elles soient sous-traitées, mais à l'exclusion des situations où les noms de domaine de premier niveau sont utilisés par un registre uniquement pour son propre usage ;

21° « entité fournissant des services d'enregistrement de noms de domaine » : un bureau d'enregistrement ou un agent agissant pour le compte de bureaux d'enregistrement, tel qu'un fournisseur ou revendeur de services d'anonymisation ou d'enregistrement fiduciaire ;

22° « 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 ;

23° « service de confiance » : un service de confiance au sens de l'article 3, point 16°, 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 ;

24° « prestataire de services de confiance » : un prestataire de services de confiance au sens de l'article 3, point 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 ;

25° « service de confiance qualifié » : un service de confiance qualifié au sens de l'article 3, point 17°, 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 ;

26° « prestataire de services de confiance qualifié » : un prestataire de services de confiance qualifié au sens de l'article 3, point 20°, 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 ;

27° « place de marché en ligne » : une place de marché en ligne au sens de l'article L. 010-1, point 15°, du Code de la consommation ;

28° « moteur de recherche en ligne » : un moteur de recherche en ligne au sens de l'article 2, point 5°, du règlement (UE) 2019/1150 du Parlement européen et du Conseil du 20 juin 2019 promouvant l'équité et la transparence pour les entreprises utilisatrices de services d'intermédiation en ligne ;

29° « service d'informatique en nuage » : un service numérique qui permet l'administration à la demande et l'accès large à distance à un ensemble modulable et variable de ressources informatiques pouvant être partagées, y compris lorsque ces ressources sont réparties à différents endroits ;

30° « service de centre de données » : un service qui englobe les structures, ou groupes de structures, dédiées à l'hébergement, l'interconnexion et l'exploitation centralisés des équipements informatiques et de réseau fournissant des services de stockage, de traitement et de transport des données, ainsi que l'ensemble des installations et infrastructures de distribution d'électricité et de contrôle environnemental ;

31° « réseau de diffusion de contenu » : un réseau de serveurs géographiquement répartis visant à assurer la haute disponibilité, l'accessibilité ou la fourniture rapide de contenu et de services numériques aux utilisateurs d'internet pour le compte de fournisseurs de contenu et de services ;

32° « plateforme de services de réseaux sociaux » : une plateforme qui permet aux utilisateurs finaux de se connecter, de partager, de découvrir et de communiquer entre eux sur plusieurs terminaux, notamment par conversations en ligne, publications, vidéos et recommandations ;

33° « représentant » : une personne physique ou morale établie dans l'Union européenne qui est expressément désignée pour agir pour le compte d'un fournisseur de services DNS, d'un registre de noms de domaine de premier niveau, d'une entité fournissant des services d'enregistrement de noms de domaine, d'un fournisseur d'informatique en nuage, d'un fournisseur de services de centre de données, d'un fournisseur de réseau de diffusion de contenu, d'un fournisseur de services gérés, d'un fournisseur de services de sécurité gérés ou d'un fournisseur de places de marché en ligne, de moteurs de recherche en ligne ou de plateformes de services de réseaux sociaux non établi dans l'Union européenne, qui peut être contactée par une autorité compétente ou un CSIRT à la place de l'entité elle-même concernant les obligations incombant à ladite entité en vertu de la présente loi ;

34° « entité de l'administration publique » : toute entité, à l'exclusion des cours et tribunaux, de la Chambre des députés et de la Banque centrale du Luxembourg, qui satisfait aux critères suivants :

a) elle a été créée pour satisfaire des besoins d'intérêt général et n'a pas de caractère industriel ou commercial ;

b) elle est dotée de la personnalité juridique ou est juridiquement habilitée à agir pour le compte d'une autre entité dotée de la personnalité juridique ;

c) elle est financée majoritairement par l'État, les autorités régionales ou d'autres organismes de droit public, sa gestion est soumise à un contrôle de la part de ces autorités ou organismes, ou son organe d'administration, de direction ou de surveillance est composé de membres dont plus de la moitié sont désignés par l'État, les autorités régionales ou d'autres organismes de droit public ;

d) elle a le pouvoir d'adresser à des personnes physiques ou morales des décisions administratives ou réglementaires affectant leurs droits en matière de mouvements transfrontières des personnes, des biens, des services ou des capitaux ;

35° « réseau de communications électroniques public » : un réseau de communications électroniques public au sens de l'article 2, point 8°, de la loi du 17 décembre 2021 sur les réseaux et les services de communications électroniques ;

36° « service de communications électroniques » : un service de communications électroniques au sens de l'article 2, point 4°, de la loi du 17 décembre 2021 sur les réseaux et les services de communications électroniques ;

37° « entité » : une personne physique ou morale constituée et reconnue comme telle en vertu du droit national de son lieu de constitution, et ayant, en son nom propre, la capacité d'être titulaire de droits et d'obligations ;

38° « fournisseur de services gérés » : une entité qui fournit des services liés à l'installation, à la gestion, à l'exploitation ou à l'entretien de produits, de réseaux, d'infrastructures ou d'applications TIC ou d'autres réseaux et systèmes d'information, par l'intermédiaire d'une assistance ou d'une administration active, soit dans les locaux des clients, soit à distance ;

39° « fournisseur de services de sécurité gérés » : un fournisseur de services gérés qui effectue ou fournit une assistance pour des activités liées à la gestion des risques en matière de cybersécurité ;

40° « organisme de recherche » : une entité dont l'objectif premier est de mener des activités de recherche appliquée ou de développement expérimental en vue d'exploiter les résultats de cette recherche à des fins commerciales, à l'exclusion des établissements d'enseignement ;

41° « CIRCL » : Computer Incident Response Center Luxembourg, opéré par le groupement d'intérêt économique Luxembourg House of Cybersecurity ;

42° « données de communications électroniques » : le contenu et les métadonnées de communications électroniques ;

43° « contenu de communications électroniques » : le contenu échangé au moyen de services de communications électroniques, notamment sous forme de texte, de voix, de documents vidéo, d'images et de son ;

44° « métadonnées de communications électroniques » : les données traitées dans un réseau de communications électroniques aux fins de la transmission, la distribution ou l'échange de contenu de communications électroniques, y compris les données permettant de retracer une communication et d'en déterminer l'origine et la destination ainsi que les données relatives à la localisation de l'appareil produites dans le cadre de la fourniture de services de communications électroniques, et la date, l'heure, la durée et le type de communication.

Chapitre 2 – Autorités en matière de cybersécurité

Art. 3. L'Institut luxembourgeois de régulation est l'autorité compétente chargée de la cybersécurité dans le cadre de la présente loi et des tâches de supervision et d'exécution visées au chapitre 6 pour les secteurs visés aux annexes I et II et les entités critiques telles que visées par la loi du XXX sur la résilience des entités critiques.

Par dérogation à l'alinéa 1er, la Commission de surveillance du secteur financier est l'autorité compétente chargée de la cybersécurité dans le cadre de la présente loi et des tâches de supervision et d'exécution visées au chapitre 6 pour le secteur bancaire et le secteur des infrastructures des marchés financiers, figurant aux points 3° et 4° du tableau de l'annexe I. Elle est par ailleurs l'autorité compétente pour le secteur des infrastructures numériques et le secteur de la gestion des services TIC, figurant aux points 8° et 9° du tableau de l'annexe I, en ce qui concerne les activités qui tombent sous la surveillance de la Commission de surveillance du secteur financier.

L'obligation au secret professionnel prévue par l'article 16 de la loi modifiée du 23 décembre 1998 portant création d'une commission de surveillance du secteur financier et l'article 15 de la loi modifiée du 30 mai 2005 portant : 1) organisation de l'Institut Luxembourgeois de Régulation ; 2) modification de la loi modifiée du 22 juin 1963 fixant le régime des traitements des fonctionnaires de l'État ne fait pas obstacle à l'échange d'informations confidentielles entre les autorités compétentes, les CSIRT et le point de contact unique tels que visés aux articles 5 et 7, dans le cadre et aux seules fins de la présente loi et des mesures prises pour son exécution.

Art. 4. L'Institut luxembourgeois de régulation bénéficie d'une contribution financière à charge du budget de l'État afin de couvrir l'intégralité des frais de fonctionnement qui résultent de l'exercice des missions prévues par la présente loi.

Art. 5. Le Haut-Commissariat à la Protection nationale constitue le point de contact unique chargé d'exercer une fonction de liaison afin d'assurer la coopération transfrontière des autorités compétentes avec les autorités compétentes des autres États membres de l'Union européenne et, le cas échéant, avec la Commission européenne et l'Agence de l'Union européenne pour la cybersécurité, ci-après « ENISA », ainsi qu'à garantir la coopération intersectorielle avec les autres autorités compétentes nationales.

Art. 6. Le Haut-Commissariat à la Protection nationale est l'autorité compétente chargée de la gestion des incidents de cybersécurité majeurs et des crises, ci-après « autorité de gestion des crises cyber » et représente le Grand-Duché de Luxembourg au sein du réseau européen pour la préparation et la gestion des crises cyber, dénommé « EU-CyCLONe », institué par l'article 16 de la directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) n° 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (directive SRI 2).

Art. 7. (1) Le Haut-Commissariat à la Protection nationale, dans sa fonction de GOVCERT.LU, constitue le centre de réponse aux incidents de sécurité informatique, ci-après « CSIRT », pour les administrations et services de l'État, les établissements publics et les entités critiques en vertu de la loi du XXX sur la résilience des entités critiques.

Le CIRCL constitue le CSIRT pour tous les autres cas, pour lesquels le Haut-Commissariat à la Protection nationale, dans sa fonction de GOVCERT.LU, n'est pas compétent.

(2) Les CSIRT couvrent au moins les secteurs, les sous-secteurs et les types d'entités visés aux annexes I et II, et sont chargés de la gestion des incidents selon un processus bien défini.

(3) Les CSIRT coopèrent et, le cas échéant, échangent des informations pertinentes conformément à l'article 19 avec des communautés sectorielles ou intersectorielles d'entités essentielles et importantes.

Art. 8. (1) Les CSIRT satisfont aux exigences suivantes :

1° ils veillent à un niveau élevé de disponibilité de leurs canaux de communication en évitant les points uniques de défaillance et disposent de plusieurs moyens pour être contactés et contacter autrui à tout moment ; ils spécifient clairement les canaux de communication et les font connaître aux partenaires et collaborateurs ;

2° leurs locaux et les systèmes d'information utilisés se trouvent sur des sites sécurisés ;

3° ils sont dotés d'un système approprié de gestion et de routage des demandes afin, notamment, de faciliter les transferts effectifs et efficaces ;

4° ~~les~~ ils garantissent la confidentialité et la fiabilité de leurs opérations ;

5° ils sont dotés des effectifs adéquats afin de pouvoir garantir une disponibilité permanente de leurs services et ils veillent à ce que leur personnel reçoive une formation appropriée ;

6° ils sont dotés de systèmes redondants et d'un espace de travail de secours pour assurer la continuité de leurs services.

Les CSIRT peuvent participer à des réseaux de coopération internationale.

(2) Les CSIRT assument les tâches suivantes :

1° surveiller et analyser les cybermenaces, les vulnérabilités et les incidents au niveau national et, sur demande, apporter une assistance aux entités essentielles et importantes concernées pour surveiller en temps réel ou quasi réel leurs réseaux et systèmes d'information ;

2° activer le mécanisme d'alerte précoce, la diffusion de messages d'alerte, les annonces et la diffusion d'informations sur les cybermenaces, les vulnérabilités et les incidents auprès des entités essentielles et importantes concernées ainsi qu'auprès des autorités compétentes et des autres parties prenantes concernées, si possible en temps quasi réel ;

3° réagir aux incidents et apporter une assistance aux entités essentielles et importantes concernées, le cas échéant ;

4° rassembler et analyser des données de police scientifique, et assurer une analyse dynamique des risques et incidents et une appréciation de la situation en matière de cybersécurité ;

5° réaliser, à la demande d'une entité essentielle ou importante, un scan proactif du réseau et des systèmes d'information de l'entité concernée afin de détecter les vulnérabilités susceptibles d'avoir un impact important ;

6° participer au réseau des CSIRT, tel que visé par la directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) n° 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (directive SRI 2) et apporter une assistance mutuelle en fonction de leurs capacités et de leurs compétences aux autres membres du réseau des CSIRT à leur demande ;

7° le cas échéant, agir en qualité de coordinateur aux fins du processus de divulgation coordonnée des vulnérabilités en vertu de l'article 9, paragraphe 1er ;

8° contribuer au déploiement d'outils de partage d'informations sécurisés conformément à l'article 10, paragraphe 3, de la directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) nº 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (directive SRI 2).

Les CSIRT peuvent procéder à un scan proactif et non intrusif des réseaux et systèmes d'information accessibles au public d'entités essentielles et importantes. Ce scan est effectué dans le but de détecter les réseaux et systèmes d'information vulnérables ou configurés de façon peu sûre et d'informer les entités concernées. Ce scan n'a pas d'effet négatif sur le fonctionnement des services des entités.

Lorsqu'ils exécutent les tâches visées à l'alinéa 1er, les CSIRT peuvent donner la priorité à certaines tâches sur la base d'une approche basée sur les risques.

(3) Les CSIRT établissent des relations de coopération avec les acteurs concernés du secteur privé, en vue d'atteindre les objectifs de la présente loi.

Art. 9. Le CIRCL est le coordinateur aux fins de la divulgation coordonnée des vulnérabilités. Il fait office d'intermédiaire de confiance en facilitant, si nécessaire, les interactions entre la personne physique ou morale qui signale une vulnérabilité et le fabricant ou le fournisseur des produits TIC ou des services TIC potentiellement vulnérables, à la demande de l'une des deux parties. Les tâches du coordinateur consistent :

1° à identifier et contacter les entités concernées ;
2° à apporter une assistance aux personnes physiques ou morales signalant une vulnérabilité ;
3° à négocier des délais de divulgation et gérer les vulnérabilités qui touchent plusieurs entités.

Les personnes physiques ou morales sont en mesure de signaler une vulnérabilité, de manière anonyme lorsqu'elles le demandent, au CIRCL. Le CIRCL veille à ce que des mesures de suivi diligentes soient prises en ce qui concerne la vulnérabilité signalée et veille à l'anonymat de la personne physique ou morale signalant la vulnérabilité. Lorsque la vulnérabilité signalée est susceptible d'avoir un impact important sur des entités dans plusieurs États membres de l'Union européenne, le CIRCL coopère, le cas échéant, avec les autres CSIRT désignés comme coordinateurs au sein du réseau des CSIRT tel que visé par la directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans

l'ensemble de l'Union, modifiant le règlement (UE) n° 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (directive SRI 2).

Art. 10. (1) Les autorités compétentes, le point de contact unique et les CSIRT coopèrent les uns avec les autres afin de respecter les obligations énoncées dans la présente loi.

(2) Les informations et notifications relatives aux incidents importants et aux incidents, aux cybermenaces et aux incidents évités notifiées à l'autorité compétente en application des articles 14 et 20, sont transmises au CSIRT concerné et au point de contact unique.

(3) Afin de veiller à ce que les tâches et obligations des autorités compétentes, du point de contact unique et des CSIRT soient exécutées efficacement, ces organes et les autorités répressives, les autorités chargées de la protection des données, les autorités nationales en vertu des règlements (CE) n° 300/2008 du Parlement européen et du Conseil du 11 mars 2008 relatif à l'instauration de règles communes dans le domaine de la sûreté de l'aviation civile et abrogeant le règlement (CE) n° 2320/2002, tel que modifié, et (UE) 2018/1139 du Parlement européen et du Conseil du 4 juillet 2018 concernant des règles communes dans le domaine de l'aviation civile et instituant une Agence de l'Union européenne pour la sécurité aérienne, et modifiant les règlements (CE) n° 2111/2005, (CE) n° 1008/2008, (UE) n° 996/2010, (UE) n° 376/2014 et les directives 2014/30/UE et 2014/53/UE du Parlement européen et du Conseil, et abrogeant les règlements (CE) n° 552/2004 et (CE) n° 216/2008 du Parlement européen et du Conseil ainsi que le règlement (CEE) n° 3922/91 du Conseil, tel que modifié, les organes de contrôle au titre du règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE, les autorités compétentes en vertu du règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) n° 1060/2009, (UE) n° 648/2012, (UE) n° 600/2014, (UE) n° 909/2014 et (UE) 2016/1011, les autorités de régulation nationales en vertu de la loi du 17 décembre 2021 sur les réseaux et les services de communications électroniques, les autorités compétentes en vertu de la loi du XXX sur la résilience des entités critiques, ainsi que les autorités compétentes en vertu d'autres actes juridiques sectoriels de l'Union européenne coopèrent de façon appropriée.

(4) Les autorités compétentes en vertu de la présente loi et les autorités compétentes en vertu de la loi du XXX sur la résilience des entités critiques coopèrent et échangent régulièrement des informations sur le recensement des entités critiques, les risques, les cybermenaces et les incidents, ainsi que sur les risques, menaces et incidents non cyber qui touchent les entités essentielles recensées en tant qu'entités critiques en vertu de la loi du XXX sur la résilience des entités critiques, et sur les mesures prises pour faire face à ces risques, menaces et incidents. Les autorités compétentes en vertu de la présente loi et les autorités compétentes en vertu 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, du règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) n° 1060/2009, (UE) n° 648/2012, (UE) n° 600/2014, (UE) n° 909/2014 et (UE) 2016/1011 et de la loi du 17 décembre 2021 sur les réseaux et les services de communications électroniques échangent régulièrement des informations pertinentes, y compris en ce qui concerne les incidents et les cybermenaces concernés.

(5) L'obligation au secret professionnel prévue par l'article 16 de la loi modifiée du 23 décembre 1998 portant création d'une commission de surveillance du secteur financier et l'article 15 de la loi modifiée du 30 mai 2005 portant : 1) organisation de l'Institut Luxembourgeois de Régulation ; 2) modification de la loi modifiée du 22 juin 1963 fixant le

régime des traitements des fonctionnaires de l'État ne fait pas obstacle aux différents types de coopération du présent article dans le cadre et aux seules fins de la présente loi et des mesures prises pour son exécution.

Chapitre 3 – Entités essentielles et importantes

Art. 11. (1) Les entités suivantes sont considérées comme étant des entités essentielles :

1° les entités d'un type visé à l'annexe I qui dépassent les plafonds applicables aux moyennes entreprises prévus à l'article 2, paragraphe 1er, de l'annexe de la recommandation 2003/361/CE de la Commission des Communautés européennes du 6 mai 2003 concernant la définition des micro, petites et moyennes entreprises ;

2° les prestataires de services de confiance qualifiés et les registres de noms de domaine de premier niveau ainsi que les fournisseurs de services DNS, quelle que soit leur taille ;

3° les fournisseurs de réseaux de communications électroniques publics ou de services de communications électroniques accessibles au public qui constituent des moyennes entreprises en vertu de l'article 2 de l'annexe de la recommandation 2003/361/CE de la Commission des Communautés européennes du 6 mai 2003 concernant la définition des micro, petites et moyennes entreprises ;

4° les entités de l'administration publique visées à l'article 1er, paragraphe 2, point 6° ;

5° toute autre entité d'un type visé à l'annexe I ou II qui est identifiée par le biais d'une décision de l'autorité compétente en tant qu'entité essentielle en vertu de l'article 1er, paragraphe 2, points 2° à 5° ;

6° les entités recensées en tant qu'entités critiques en vertu de la loi du XXX sur la résilience des entités critiques, visées à l'article 1er, paragraphe 3 ;

7° les entités que les autorités compétentes ont identifiées avant l'entrée en vigueur de la présente loi comme des opérateurs de services essentiels conformément à la loi du 28 mai 2019 portant transposition de la directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union européenne et modifiant 1° la loi modifiée du 20 avril 2009 portant création du Centre des technologies de l'information de l'État et 2° la loi du 23 juillet 2016 portant création d'un Haut-Commissariat à la Protection nationale.

(2) Aux fins de la présente loi, les entités d'un type visé à l'annexe I ou II qui ne constituent pas des entités essentielles en vertu du paragraphe 1er du présent article sont considérées comme des entités importantes. Celles-ci incluent les entités identifiées par l'autorité compétente en tant qu'entités importantes en vertu de l'article 1er, paragraphe 2, points 2° à 5°.

(3) Les autorités compétentes établissent une liste des entités essentielles et importantes ainsi que des entités fournissant des services d'enregistrement de noms de domaine. Les autorités compétentes réexaminent cette liste et, le cas échéant, la mettent à jour régulièrement et au moins tous les deux ans par la suite. Ces listes sont transmises par l'autorité compétente au CSIRT compétent et au point de contact unique.

(4) Aux fins de l'établissement de la liste visée au paragraphe 3, les entités visées audit paragraphe communiquent aux autorités compétentes, dans un délai de deux mois à compter de l'entrée en vigueur de la présente loi, au moins les informations suivantes :

1° le nom de l'entité ;

2° l'adresse et les coordonnées actualisées, y compris les adresses électroniques, les plages d'IP et les numéros de téléphone ;

3° le cas échéant, le secteur et le sous-secteur concernés visés à l'annexe I ou II ;

4° le cas échéant, une liste des États membres de l'Union européenne dans lesquels elles fournissent des services relevant du champ d'application de la présente loi ;

5° la taille de l'entité et, le cas échéant, celle du groupe d'entités auquel l'entité concernée appartient.

Les entités visées au paragraphe 3 notifient sans tarder toute modification des informations qu'elles ont communiquées conformément à l'alinéa 1er du présent paragraphe et, en tout état de cause, dans un délai de deux semaines à compter de la date de la modification.

Les autorités compétentes mettent en place des mécanismes nationaux permettant aux entités de s'enregistrer elles-mêmes. L'autorité compétente concernée confirme à ces entités concernées leur désignation en tant qu'entité essentielle ou importante.

Art. 12. (1) Les entités essentielles et importantes prennent les mesures techniques, opérationnelles et organisationnelles appropriées et proportionnées pour gérer les risques qui menacent la sécurité des réseaux et des systèmes d'information que ces entités utilisent dans le cadre de leurs activités ou de la fourniture de leurs services, ainsi que pour éliminer ou réduire les conséquences que les incidents ont sur les destinataires de leurs services et sur d'autres services.

Les mesures visées à l'alinéa 1er garantissent, pour les réseaux et les systèmes d'information, un niveau de sécurité adapté au risque existant, en tenant compte de l'état des connaissances et, s'il y a lieu, des normes européennes et internationales applicables, ainsi que du coût de mise en œuvre. Lors de l'évaluation de la proportionnalité de ces mesures, il convient de tenir dûment compte du degré d'exposition de l'entité aux risques, de la taille de l'entité et de la probabilité de survenance d'incidents et de leur gravité, y compris leurs conséquences sociétales et économiques.

Afin d'identifier les risques, les entités essentielles et importantes utilisent un cadre d'analyse de risques approprié pouvant être précisé par l'autorité compétente concernée par voie de règlement ou de circulaire.

(2) Les mesures visées au paragraphe 1er sont fondées sur une approche « tous risques » qui vise à protéger les réseaux et les systèmes d'information ainsi que leur environnement physique contre les incidents, et elles comprennent au moins :

1° les politiques relatives à l'analyse des risques et à la sécurité des systèmes d'information ;

2° la gestion des incidents ;

3° la continuité des activités, par exemple la gestion des sauvegardes et la reprise des activités, et la gestion des crises ;

4° la sécurité de la chaîne d'approvisionnement, y compris les aspects liés à la sécurité concernant les relations entre chaque entité et ses fournisseurs ou prestataires de services directs ;

5° la sécurité de l'acquisition, du développement et de la maintenance des réseaux et des systèmes d'information, y compris le traitement et la divulgation des vulnérabilités ;

6° des politiques et des procédures pour évaluer l'efficacité des mesures de gestion des risques en matière de cybersécurité ;

7° les pratiques de base en matière de cyberhygiène et la formation à la cybersécurité ;

8° des politiques et des procédures relatives à l'utilisation de la cryptographie et, le cas échéant, du chiffrement ;

9° la sécurité des ressources humaines, des politiques de contrôle d'accès et la gestion des actifs ;

10° l'utilisation de solutions d'authentification à plusieurs facteurs ou d'authentification continue, de communications vocales, vidéo et textuelles sécurisées et de systèmes sécurisés de communication d'urgence au sein de l'entité, selon les besoins.

(3) Les mesures prises par les entités essentielles sur base des paragraphes 1er et 2 sont notifiées à l'autorité compétente. Les modalités de cette notification, le format et le délai, sont déterminées par l'autorité compétente concernée par voie de règlement ou de circulaire.

(4) Les autorités compétentes veillent à ce que, lorsqu'elles examinent lesquelles des mesures visées au paragraphe 2, point 4°, du présent article sont appropriées, les entités tiennent compte des vulnérabilités propres à chaque fournisseur et prestataire de services direct et de la qualité globale des produits et des pratiques de cybersécurité de leurs fournisseurs et prestataires de services, y compris de leurs procédures de développement sécurisé. Les autorités compétentes veillent également à ce que, lorsqu'elles examinent lesquelles des mesures visées audit point sont appropriées, les entités soient tenues de prendre en compte les résultats des évaluations coordonnées des risques pour la sécurité des chaînes d'approvisionnement critiques, effectuées conformément à l'article 22, paragraphe 1er, de la directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) n° 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (directive SRI 2).

(5) Les autorités compétentes veillent à ce que, lorsqu'une entité constate qu'elle ne se conforme pas aux mesures prévues au paragraphe 2, elle prenne, sans retard injustifié, toutes les mesures correctives nécessaires appropriées et proportionnées.

Art. 13. (1) Les organes de direction des entités essentielles et importantes approuvent les mesures de gestion des risques en matière de cybersécurité prises par ces entités afin de se conformer à l'article 12, supervisent leur mise en œuvre et peuvent être tenus responsables de la violation dudit article par ces entités.

(2) Les membres des organes de direction des entités essentielles et importantes sont tenus de suivre régulièrement une formation et les entités essentielles et importantes offrent régulièrement une formation similaire aux membres de leur personnel afin que ceux-ci acquièrent des connaissances et des compétences suffisantes pour déterminer les risques et

évaluer les pratiques de gestion des risques en matière de cybersécurité et leur impact sur les services fournis par l'entité.

Art. 14. (1) Les entités essentielles et importantes notifient, sans retard injustifié, à l'autorité compétente concernée, conformément au paragraphe 4, tout incident ayant un impact important sur leur fourniture des services visé au paragraphe 3, ci-après « incident important ». Le cas échéant, les entités concernées notifient, sans retard injustifié, aux destinataires de leurs services les incidents importants susceptibles de nuire à la fourniture de ces services. Ces entités signalent, entre autres, toute information permettant à l'autorité compétente de déterminer si l'incident a un impact transfrontière. Le simple fait de notifier un incident n'accroît pas la responsabilité de l'entité qui est à l'origine de la notification.

L'autorité compétente transmet la notification au CSIRT concerné et au point de contact unique dès qu'elle la reçoit.

(2) Le cas échéant, les entités essentielles et importantes communiquent, sans retard injustifié, aux destinataires de leurs services qui sont potentiellement affectés par une cybermenace importante toutes les mesures ou corrections que ces destinataires peuvent appliquer en réponse à cette menace. Le cas échéant, les entités informent également ces destinataires de la cybermenace importante elle-même.

(3) Un incident est considéré comme important si :

1° il a causé ou est susceptible de causer une perturbation opérationnelle grave des services ou des pertes financières pour l'entité concernée ;

2° il a affecté ou est susceptible d'affecter d'autres personnes physiques ou morales en causant des dommages matériels, corporels ou moraux considérables.

L'autorité compétente concernée peut préciser, par voie de règlement ou de circulaire, les paramètres et les modalités des notifications des incidents ayant un impact important sur leur fourniture des services.

(4) Aux fins de la notification visée au paragraphe 1er, les entités concernées soumettent à l'autorité compétente :

1° sans retard injustifié et en tout état de cause dans les vingt-quatre heures après avoir eu connaissance de l'incident important, une notification préliminaire qui, le cas échéant, indique si l'on suspecte l'incident important d'avoir été causé par des actes illicites ou malveillants ou s'il pourrait avoir un impact transfrontière ;

2° sans retard injustifié et en tout état de cause dans les soixante-douze heures après avoir eu connaissance de l'incident important, une notification d'incident qui, le cas échéant, met à jour les informations visées au point 1° et fournit une évaluation initiale de l'incident important, y compris de sa gravité et de son impact, ainsi que des indicateurs de compromission, lorsqu'ils sont disponibles ;

3° à la demande d'un CSIRT ou, selon le cas, de l'autorité compétente, un rapport intermédiaire sur les mises à jour pertinentes de la situation ;

4° un rapport final au plus tard un mois après la présentation de la notification d'incident visée au point 2°, comprenant les éléments suivants :

a) une description détaillée de l'incident, y compris de sa gravité et de son impact ;

b) le type de menace ou la cause profonde qui a probablement déclenché l'incident ;

c) les mesures d'atténuation appliquées et en cours ;

d) le cas échéant, l'impact transfrontière de l'incident ;

5° en cas d'incident en cours au moment de la présentation du rapport final visé au point 4°, les entités concernées fournissent à ce moment-là un rapport d'avancement puis un rapport final dans un délai d'un mois à compter de la gestion de l'incident.

Par dérogation à l'alinéa 1er, point 2°, un prestataire de services de confiance notifie à l'autorité compétente les incidents importants qui ont un impact sur la fourniture de ses services de confiance, sans retard injustifié et en tout état de cause dans les vingt-quatre heures après avoir eu connaissance de l'incident important.

(5) L'autorité compétente fournit, sans retard injustifié et si possible dans les vingt-quatre heures suivant la réception de la notification préliminaire visée au paragraphe 4, point 1°, une réponse à l'entité émettrice de la notification, y compris un retour d'information initial sur l'incident important et, à la demande de l'entité, des orientations ou des conseils opérationnels sur la mise en œuvre d'éventuelles mesures d'atténuation. L'orientation est émise par l'autorité compétente en coopération avec le CSIRT concerné. Le CSIRT fournit un soutien technique supplémentaire si l'entité concernée le demande. Lorsqu'il y a lieu de suspecter que l'incident est de nature criminelle, le CSIRT ou l'autorité compétente fournit également des orientations sur les modalités de notification de l'incident important aux autorités répressives.

(6) Lorsque c'est approprié, et notamment si l'incident important concerne deux États membres de l'Union européenne ou plus, le point de contact unique informe, sans retard injustifié, les autres États membres de l'Union européenne touchés et l'ENISA de l'incident important. Sont alors partagées des informations du type de celles reçues conformément au paragraphe 4. Ce faisant, le point de contact unique doit préserver la sécurité et les intérêts commerciaux de l'entité ainsi que la confidentialité des informations communiquées.

(7) Lorsque la sensibilisation du public est nécessaire pour prévenir un incident important ou pour faire face à un incident important en cours, ou lorsque la divulgation de l'incident important est par ailleurs dans l'intérêt public, l'autorité compétente et, le cas échéant, les CSIRT ou les autorités compétentes des autres États membres de l'Union européenne concernés peuvent, après avoir consulté l'entité concernée, informer le public de l'incident important ou exiger de l'entité qu'elle le fasse.

(8) À la demande de l'autorité compétente, le point de contact unique transmet les notifications reçues en vertu du paragraphe 1er aux points de contact uniques des autres États membres de l'Union européenne touchés.

(9) Le point de contact unique soumet tous les trois mois à l'ENISA un rapport de synthèse comprenant des données anonymisées et agrégées sur les incidents importants, les incidents, les cybermenaces et les incidents évités notifiés conformément au paragraphe 1er et à l'article 20.

(10) L'autorité compétente fournit aux autorités compétentes en vertu de la loi du XXX sur la résilience des entités critiques des informations sur les incidents importants, les incidents, les cybermenaces et les incidents évités notifiés conformément au paragraphe 1er et à l'article 20 par les entités identifiées comme des entités critiques en vertu de la loi du XXX sur la résilience des entités critiques.

Art. 15. Afin de démontrer la conformité à certaines exigences visées à l'article 12, l'autorité compétente peut prescrire, par voie de règlement et en prenant en considération les actes délégués adoptés par la Commission européenne en vertu de l'article 24, paragraphe 2, de la directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) n° 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (directive SRI 2), aux entités essentielles et importantes d'utiliser des produits TIC, services TIC et processus TIC particuliers qui, mis au point par l'entité essentielle ou importante ou acquis auprès de tiers, sont certifiés dans le cadre de schémas européens de certification de cybersécurité adoptés conformément à l'article 49 du règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) n° 526/2013 (règlement sur la cybersécurité), tel que modifié. En outre, l'autorité compétente encourage les entités essentielles et importantes à utiliser des services de confiance qualifiés.

Chapitre 4 – Compétence et enregistrement

Art. 16. (1) Les entités relevant du champ d'application de la présente loi sont considérées comme relevant de la compétence du Grand-Duché de Luxembourg lorsqu'elles y sont établies, à l'exception des cas suivants :

1° les fournisseurs de réseaux de communications électroniques publics ou les fournisseurs de services de communications électroniques accessibles au public, qui sont considérés comme relevant de la compétence de l'État membre de l'Union européenne dans lequel ils fournissent leurs services ;

2° les fournisseurs de services DNS, les registres des noms de domaine de premier niveau, les entités fournissant des services d'enregistrement de noms de domaine, les fournisseurs de services d'informatique en nuage, les fournisseurs de services de centres de données, les fournisseurs de réseaux de diffusion de contenu, les fournisseurs de services gérés, les fournisseurs de services de sécurité gérés, ainsi que les fournisseurs de places de marché en ligne, de moteurs de recherche en ligne ou de plateformes de services de réseaux sociaux, qui sont considérés comme relevant de la compétence de l'État membre de l'Union européenne dans lequel ils ont leur établissement principal dans l'Union européenne en application du paragraphe 2 ;

3° les entités de l'administration publique, qui sont considérées comme relevant de la compétence de l'État membre de l'Union européenne qui les a établies.

(2) Aux fins de la présente loi, une entité visée au paragraphe 1er, point 2°, est considérée avoir son établissement principal dans l'Union européenne dans l'État membre où sont principalement prises les décisions relatives aux mesures de gestion des risques en matière de cybersécurité. Si un tel État membre de l'Union européenne ne peut être déterminé ou si ces décisions ne sont pas prises dans l'Union européenne, l'établissement principal est considéré comme se trouvant dans l'État membre de l'Union européenne où les opérations de cybersécurité sont effectuées. Si un tel État membre de l'Union européenne ne peut être déterminé, l'établissement principal est considéré comme se trouvant dans l'État membre de l'Union européenne où l'entité concernée possède l'établissement comptant le plus grand nombre de salariés dans l'Union européenne.

(3) Si une entité visée au paragraphe 1er, point 2°, n'est pas établie dans l'Union européenne mais offre des services sur le territoire du Grand-Duché de Luxembourg, elle désigne un représentant dans l'Union européenne. Le représentant est établi dans l'un des États

membres de l'Union européenne dans lesquels les services sont fournis. Une telle entité est considérée comme relevant de la compétence du Grand-Duché de Luxembourg si le représentant y est établi. En l'absence d'un représentant dans l'Union européenne désigné en vertu du présent paragraphe et si l'entité fournit des services au Grand-Duché de Luxembourg, l'autorité compétente peut assigner l'entité à comparaître devant le président du Tribunal d'arrondissement de Luxembourg statuant comme en matière de référé aux fins d'ordonner la désignation d'un représentant dans l'Union européenne.

(4) La désignation d'un représentant par une entité visée au paragraphe 1er, point 2°, est sans préjudice d'actions en justice qui pourraient être intentées contre l'entité elle-même.

(5) L'autorité compétente qui a reçu une demande d'assistance mutuelle en lien avec une entité visée au paragraphe 1er, point 2°, peut, dans les limites de cette demande, prendre des mesures de supervision et d'exécution appropriées à l'égard de l'entité concernée qui fournit des services ou qui dispose d'un réseau et d'un système d'information sur le territoire luxembourgeois.

Art. 17. (1) Les fournisseurs de services DNS, les registres des noms de domaine de premier niveau, les entités fournissant des services d'enregistrement de noms de domaine, les fournisseurs de services d'informatique en nuage, les fournisseurs de services de centres de données, les fournisseurs de réseaux de diffusion de contenu, les fournisseurs de services gérés, les fournisseurs de services de sécurité gérés, ainsi que les fournisseurs de places de marché en ligne, de moteurs de recherche en ligne ou de plateformes de services de réseaux sociaux soumettent les informations suivantes à l'autorité compétente au plus tard le 17 janvier 2025 :

1° le nom de l'entité ;

2° les secteur, sous-secteur et type d'entité concernés, visés à l'annexe I ou II, le cas échéant ;

3° l'adresse de l'établissement principal de l'entité et de ses autres établissements légaux dans l'Union européenne ou, si elle n'est pas établie dans l'Union européenne, de son représentant désigné conformément à l'article 16, paragraphe 3 ;

4° les coordonnées actualisées, y compris les adresses de courrier électronique et les numéros de téléphone de l'entité et, le cas échéant, de son représentant désigné conformément à l'article 16, paragraphe 3 ;

5° les États membres de l'Union européenne dans lesquels l'entité fournit des services ;

6° les plages d'IP de l'entité.

Le point de contact unique transmet ces informations, à l'exception de celles visées au paragraphe 1er, point 6°, à l'ENISA, afin de permettre à l'ENISA de mettre en place le registre visé à l'article 27 de la directive 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) n° 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (directive SRI 2).

(2) Les entités visées au paragraphe 1er notifient à l'autorité compétente toute modification des informations qu'elles ont communiquées en vertu dudit paragraphe sans tarder et, en tout état de cause, dans un délai de trois mois à compter de la date de la modification.

Art. 18. (1) Afin de contribuer à la sécurité, à la stabilité et à la résilience du DNS, les registres des noms de domaine de premier niveau et les entités fournissant des services d'enregistrement de noms de domaine collectent les données d'enregistrement de noms de domaine et les maintiennent exactes et complètes au sein d'une base de données spécialisée avec la diligence requise par la législation sur la protection des données à caractère personnel.

(2) Aux fins du paragraphe 1er, la base de données d'enregistrement des noms de domaine contient les informations nécessaires pour identifier et contacter les titulaires des noms de domaine et les points de contact qui gèrent les noms de domaine relevant des domaines de premier niveau. Ces informations comprennent notamment les éléments suivants :

1° le nom de domaine ;

2° la date d'enregistrement ;

3° le nom du titulaire, l'adresse de courrier électronique et le numéro de téléphone permettant de le contacter ;

4° l'adresse de courrier électronique et le numéro de téléphone permettant de contacter le point de contact qui gère le nom de domaine, si ces coordonnées sont différentes de celles du titulaire.

(3) Les registres des noms de domaine de premier niveau et les entités fournissant des services d'enregistrement de noms de domaine mettent en place des politiques et des procédures, notamment des procédures de vérification, visant à garantir que les bases de données visées au paragraphe 1er contiennent des informations exactes et complètes. Ces politiques et procédures sont mises à la disposition du public.

(4) Les registres des noms de domaine de premier niveau et les entités fournissant des services d'enregistrement de noms de domaine rendent publiques, sans retard injustifié après l'enregistrement d'un nom de domaine, les données d'enregistrement du nom de domaine qui ne sont pas des données à caractère personnel.

(5) Les registres des noms de domaine de premier niveau et les entités fournissant des services d'enregistrement de noms de domaine donnent accès aux données spécifiques d'enregistrement de noms de domaine sur demande légitime et dûment motivée des demandeurs d'accès légitimes, dans le respect de la législation sur la protection des données. Les registres des noms de domaine de premier niveau et les entités fournissant des services d'enregistrement de noms de domaine répondent sans retard injustifié et, en tout état de cause, dans un délai de soixante-douze heures après réception de toute demande d'accès. Les politiques et procédures de divulgation de ces données sont rendues publiques.

(6) Le respect des obligations énoncées aux paragraphes 1er à 5 ne saurait entraîner de répétition inutile de la collecte des données d'enregistrement de noms de domaines. À cet effet, les registres des noms de domaine de premier niveau et les entités fournissant des services d'enregistrement de noms de domaine coopèrent entre eux.

Chapitre 5 – Partage d'informations

Art. 19. (1) Les entités relevant du champ d'application de la présente loi et, le cas échéant, les autres entités concernées ne relevant pas du champ d'application de la présente loi peuvent échanger entre elles, à titre volontaire, des informations pertinentes en matière de cybersécurité, y compris des informations relatives aux cybermenaces, aux incidents évités,

aux vulnérabilités, aux techniques et procédures, aux indicateurs de compromission, aux tactiques adverses, ainsi que des informations spécifiques sur les acteurs de la menace, des alertes de cybersécurité et des recommandations concernant la configuration des outils de cybersécurité pour détecter les cyberattaques, lorsque ce partage d'informations :

1° vise à prévenir et à détecter les incidents, à y réagir, à s'en rétablir ou à atténuer leur impact ;

2° renforce le niveau de cybersécurité, notamment en sensibilisant aux cybermenaces, en limitant ou en empêchant leur capacité de se propager, en soutenant une série de capacités de défense, en remédiant aux vulnérabilités et en les révélant, en mettant en œuvre des techniques de détection, d'endiguement et de prévention des menaces, des stratégies d'atténuation ou des étapes de réaction et de rétablissement, ou en encourageant la recherche collaborative en matière de cybermenaces entre les entités publiques et privées.

(2) Cet échange d'informations a lieu au sein de communautés d'entités essentielles et importantes ainsi que, le cas échéant, de leurs fournisseurs ou prestataires de services et est mis en œuvre au moyen d'accords de partage d'informations en matière de cybersécurité, compte tenu de la nature potentiellement sensible des informations partagées.

(3) Les entités essentielles et importantes notifient à l'autorité compétente leur participation aux accords de partage d'informations en matière de cybersécurité visés au paragraphe 2, lorsqu'elles concluent de tels accords ou, le cas échéant, lorsqu'elles se retirent de ces accords, une fois que le retrait prend effet.

Art. 20. (1) Outre l'obligation de notification prévue à l'article 14, des notifications peuvent être transmises à titre volontaire :

1° aux autorités compétentes par les entités essentielles et importantes en ce qui concerne les incidents, les cybermenaces et les incidents évités ;

2° à l'Institut luxembourgeois de régulation par les entités autres que celles visées au point 1°, indépendamment du fait qu'elles relèvent ou non du champ d'application de la présente loi, en ce qui concerne les incidents importants, les cybermenaces ou les incidents évités.

(2) L'autorité compétente traite les notifications visées au paragraphe 1er conformément à la procédure énoncée à l'article 14. L'autorité compétente peut traiter les notifications obligatoires en leur donnant la priorité par rapport aux notifications volontaires.

Lorsque cela est nécessaire, l'autorité compétente fournit au CSIRT concerné et au point de contact unique les informations relatives aux notifications reçues en vertu du présent article, tout en garantissant la confidentialité et une protection appropriée des informations fournies par l'entité à l'origine de la notification. Sans préjudice de la prévention et de la détection d'infractions pénales et des enquêtes et poursuites en la matière, un signalement volontaire n'a pas pour effet d'imposer à l'entité ayant effectué la notification des obligations supplémentaires auxquelles elle n'aurait pas été soumise si elle n'avait pas transmis la notification.

Chapitre 6 – Supervision et exécution

Art. 21. (1) Lorsque les autorités compétentes accomplissent leurs tâches de supervision prévues aux articles 22 et 23, elles peuvent mettre au point des méthodes de supervision

permettant de fixer des priorités concernant ces tâches selon une approche basée sur les risques.

(2) Lorsqu'elles traitent des incidents donnant lieu à des violations de données à caractère personnel, les autorités compétentes coopèrent étroitement avec les autorités de contrôle 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 abrogeant la directive 95/46/CE (règlement général sur la protection des données), tel que modifié, sans préjudice de la compétence et des missions des autorités de contrôle.

Art. 22. (1) Les mesures de supervision ou d'exécution imposées aux entités essentielles à l'égard des obligations prévues par la présente loi doivent être effectives, proportionnées et dissuasives, compte tenu des circonstances de chaque cas.

(2) Les autorités compétentes, lorsqu'elles accomplissent leurs tâches de supervision à l'égard d'entités essentielles, ont le pouvoir de soumettre ces entités à :

1° des inspections sur place et des contrôles à distance, y compris des contrôles aléatoires effectués par des professionnels formés ;

2° des audits de sécurité réguliers et ciblés réalisés par un organisme indépendant ou l'autorité compétente ;

3° des audits ad hoc, notamment lorsqu'ils sont justifiés en raison d'un incident important ou d'une violation de la présente loi par l'entité essentielle ;

4° des scans de sécurité fondés sur des critères d'évaluation des risques objectifs, non discriminatoires, équitables et transparents, si nécessaire avec la coopération de l'entité concernée ;

5° des demandes d'informations nécessaires à l'évaluation des mesures de gestion des risques en matière de cybersécurité adoptées par l'entité concernée, notamment les politiques de cybersécurité consignées par écrit, ainsi que du respect de l'obligation de soumettre des informations aux autorités compétentes conformément à l'article 17 ;

6° des demandes d'accès à des données, à des documents et à toutes informations nécessaires à l'accomplissement de leurs tâches de supervision ;

7° des demandes de preuves de la mise en œuvre de politiques de cybersécurité, telles que les résultats des audits de sécurité effectués par un auditeur qualifié et les éléments de preuve sous-jacents correspondants.

Les audits de sécurité ciblés visés à l'alinéa 1er, point 2°, sont basés sur des évaluations des risques effectuées par l'autorité compétente ou l'entité contrôlée, ou sur d'autres informations disponibles relatives aux risques.

Les résultats de tout audit de sécurité ciblé sont mis à la disposition de l'autorité compétente. Les coûts de cet audit de sécurité ciblé effectué par un organisme indépendant sont à la charge de l'entité contrôlée, sauf lorsque l'autorité compétente en décide autrement dans des cas dûment motivés.

(3) Lorsqu'elles exercent leurs pouvoirs en vertu du paragraphe 2, points 5°, 6° ou 7°, les autorités compétentes mentionnent la finalité de la demande et précisent quelles sont les informations exigées.

(4) Les autorités compétentes, lorsqu'elles exercent leurs pouvoirs d'exécution à l'égard d'entités essentielles, ont le pouvoir :

1° d'émettre des avertissements concernant les violations de la présente loi par les entités concernées ;

2° d'adopter des instructions contraignantes, y compris en ce qui concerne les mesures nécessaires pour éviter un incident ou y remédier, ainsi que les délais pour mettre en œuvre ces mesures et rendre compte de cette mise en œuvre, ou une injonction exigeant des entités concernées qu'elles remédient aux insuffisances constatées ou aux violations de la présente loi ;

3° d'ordonner aux entités concernées de mettre un terme à un comportement qui viole la présente loi et de ne pas le réitérer ;

4° d'ordonner aux entités concernées de garantir la conformité de leurs mesures de gestion des risques en matière de cybersécurité avec l'article 12 ou de respecter les obligations d'information énoncées à l'article 14, de manière spécifique et dans un délai déterminé ;

5° d'ordonner aux entités concernées d'informer les personnes physiques ou morales à l'égard desquelles elles fournissent des services ou exercent des activités susceptibles d'être affectés par une cybermenace importante de la nature de la menace, ainsi que de toutes mesures préventives ou réparatrices que ces personnes physiques ou morales pourraient prendre en réponse à cette menace ;

6° d'ordonner aux entités concernées de mettre en œuvre les recommandations formulées à la suite d'un audit de sécurité dans un délai raisonnable ;

7° de désigner, pour une période déterminée, un responsable du contrôle ayant des tâches bien définies pour superviser le respect, par les entités concernées, des articles 12 et 14 ;

8° d'ordonner aux entités concernées de rendre publics les aspects de violations de la présente loi de manière spécifique ;

9° d'imposer une amende administrative en vertu de l'article 26 en plus de l'une ou l'autre des mesures visées aux points 1° à 8° du présent paragraphe.

(5) Lorsque les mesures d'exécution adoptées en vertu du paragraphe 4, points 1° à 4° et point 6°, sont inefficaces, les autorités compétentes peuvent fixer un délai dans lequel l'entité essentielle est invitée à prendre les mesures nécessaires pour pallier les insuffisances ou satisfaire aux exigences de ces autorités. Si la mesure demandée n'est pas prise dans le délai imparti, les autorités compétentes ont le pouvoir :

1° de demander au président du Tribunal d'arrondissement de Luxembourg statuant comme en matière de référé de suspendre temporairement une certification ou une autorisation concernant tout ou partie des services pertinents fournis ou des activités pertinentes menées par l'entité essentielle ;

2° de demander au président du Tribunal d'arrondissement de Luxembourg statuant comme en matière de référé d'interdire temporairement à toute personne physique

exerçant des responsabilités dirigeantes à un niveau de directeur général ou de représentant légal dans l'entité essentielle d'exercer des responsabilités dirigeantes dans cette entité.

Les suspensions ou interdictions temporaires imposées au titre du présent paragraphe sont uniquement appliquées jusqu'à ce que l'entité concernée prenne les mesures nécessaires pour remédier aux insuffisances ou se conformer aux exigences de l'autorité compétente à l'origine de l'application de ces mesures d'exécution. La mainlevée de ces suspensions ou interdictions temporaires est prononcée par le président du Tribunal d'arrondissement de Luxembourg statuant comme en matière de référé.

Les mesures d'exécution prévues au présent paragraphe ne peuvent pas être appliquées aux entités de l'administration publique qui relèvent de la présente loi.

(6) Toute personne physique responsable d'une entité essentielle ou agissant en qualité de représentant légal d'une entité essentielle sur la base du pouvoir de la représenter, de prendre des décisions en son nom ou d'exercer son contrôle a le pouvoir de veiller au respect, par l'entité, de la présente loi. Ces personnes physiques peuvent être tenues responsables des manquements à leur devoir de veiller au respect de la présente loi.

En ce qui concerne les entités de l'administration publique, le présent paragraphe est sans préjudice du droit national en ce qui concerne la responsabilité des agents de la fonction publique et des responsables élus ou nommés.

(7) Lorsqu'elles prennent toute mesure d'exécution visée au paragraphe 4 ou 5, les autorités compétentes respectent les droits de la défense et tiennent compte des circonstances propres à chaque cas et, au minimum, tiennent dûment compte :

1° de la gravité de la violation et de l'importance des dispositions enfreintes, les faits suivants, entre autres, devant être considérés en tout état de cause comme graves :

a) les violations répétées ;

b) le fait de ne pas notifier des incidents importants ou de ne pas y remédier ;

c) le fait de ne pas pallier les insuffisances à la suite d'instructions contraignantes des autorités compétentes ;

d) le fait d'entraver des audits ou des activités de contrôle ordonnées par l'autorité compétente à la suite de la constatation d'une violation ;

e) la fourniture d'informations fausses ou manifestement inexactes relatives aux mesures de gestion des risques en matière de cybersécurité ou aux obligations d'information prévues aux articles 12 et 14 ;

2° de la durée de la violation ;

3° de toute violation antérieure pertinente commise par l'entité concernée ;

4° des dommages matériels, corporels ou moraux causés, y compris des pertes financières ou économiques, des effets sur d'autres services et du nombre d'utilisateurs touchés ;

5° du fait que l'auteur de la violation a agi délibérément ou par négligence ;

6° des mesures prises par l'entité pour prévenir ou atténuer les dommages matériels, corporels ou moraux ;

7° de l'application de codes de conduite approuvés ou de mécanismes de certification approuvés ;

8° du degré de coopération avec les autorités compétentes des personnes physiques ou morales tenues pour responsables.

(8) Les autorités compétentes exposent en détail les motifs de leurs mesures d'exécution. Avant de prendre de telles mesures, les autorités compétentes informent les entités concernées de leurs conclusions préliminaires. Elles laissent en outre à ces entités un délai raisonnable pour communiquer leurs observations, sauf dans des cas exceptionnels dûment motivés où cela empêcherait une intervention immédiate pour prévenir un incident ou y répondre.

(9) Les autorités compétentes en vertu de la présente loi informent les autorités compétentes concernées en vertu de la loi du XXX sur la résilience des entités critiques lorsqu'elles exercent leurs pouvoirs de supervision et d'exécution dans le but de garantir qu'une entité définie comme critique en vertu de la loi du XXX sur la résilience des entités critiques respecte la présente loi. S'il y a lieu, les autorités compétentes en vertu de la loi du XXX sur la résilience des entités critiques peuvent demander aux autorités compétentes en vertu de la présente loi d'exercer leurs pouvoirs de supervision et d'exécution à l'égard d'une entité qui est définie comme entité critique en vertu de la loi du XXX sur la résilience des entités critiques.

(10) Les autorités compétentes en vertu de la présente loi coopèrent avec les autorités compétentes pertinentes de l'État membre de l'Union européenne concerné au titre du règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) n° 1060/2009, (UE) n° 648/2012, (UE) n° 600/2014, (UE) n° 909/2014 et (UE) 2016/1011. Les autorités compétentes en vertu de la présente loi informent le forum de supervision institué en vertu de l'article 32, paragraphe 1er, du règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) n° 1060/2009, (UE) n° 648/2012, (UE) n° 600/2014, (UE) n° 909/2014 et (UE) 2016/1011 lorsqu'elles exercent leurs pouvoirs de supervision et d'exécution dans le but de garantir qu'une entité essentielle qui a été désignée comme étant un prestataire tiers critique de services TIC au titre de l'article 31 dudit règlement respecte la présente loi.

Art. 23. (1) Au vu d'éléments de preuve, d'indications ou d'informations selon lesquels une entité importante ne respecterait pas la présente loi, et notamment ses articles 12 et 14, les autorités compétentes prennent des mesures, le cas échéant, dans le cadre de mesures de contrôle ex post. Ces mesures doivent être effectives, proportionnées et dissuasives, compte tenu des circonstances propres à chaque cas d'espèce.

(2) Les autorités compétentes, lorsqu'elles accomplissent leurs tâches de supervision à l'égard d'entités importantes, ont le pouvoir de soumettre ces entités à :

1° des inspections sur place et des contrôles à distance ex post, effectués par des professionnels formés ;

2° des audits de sécurité ciblés réalisés par un organisme indépendant ou l'autorité compétente ;

3° des scans de sécurité fondés sur des critères d'évaluation des risques objectifs, non discriminatoires, équitables et transparents, si nécessaire avec la coopération de l'entité concernée ;

4° des demandes d'informations nécessaires à l'évaluation ex post des mesures de gestion des risques en matière de cybersécurité adoptées par l'entité concernée, notamment les politiques de cybersécurité consignées par écrit, ainsi que du respect de l'obligation de soumettre des informations aux autorités compétentes conformément à l'article 17 ;

5° des demandes d'accès à des données, à des documents et à des informations nécessaires à l'accomplissement de leurs tâches de supervision ;

6° des demandes de preuves de la mise en œuvre de politiques de cybersécurité, telles que les résultats des audits de sécurité effectués par un auditeur qualifié et les éléments de preuve sous-jacents correspondants.

Les audits de sécurité ciblés visés à l'alinéa 1er, point 2°, sont fondés sur des évaluations des risques effectuées par l'autorité compétente ou l'entité contrôlée, ou sur d'autres informations disponibles relatives aux risques.

Les résultats de tout audit de sécurité ciblé sont mis à la disposition de l'autorité compétente. Les coûts de cet audit de sécurité ciblé effectué par un organisme indépendant sont à la charge de l'entité contrôlée, sauf lorsque l'autorité compétente en décide autrement dans des cas dûment motivés.

(3) Lorsqu'elles exercent leurs pouvoirs en vertu du paragraphe 2, points 4°, 5° ou 6°, les autorités compétentes mentionnent la finalité de la demande et précisent quelles sont les informations exigées.

(4) Les autorités compétentes, lorsqu'elles exercent leurs pouvoirs d'exécution à l'égard d'entités importantes, ont le pouvoir :

1° d'émettre des avertissements concernant des violations de la présente loi par les entités concernées ;

2° d'adopter des instructions contraignantes ou une injonction exigeant des entités concernées qu'elles pallient les insuffisances constatées ou les violations de la présente loi ;

3° d'ordonner aux entités concernées de mettre un terme à un comportement qui viole la présente loi et de ne pas le réitérer ;

4° d'ordonner aux entités concernées de garantir la conformité de leurs mesures de gestion des risques en matière de cybersécurité avec l'article 12 ou de respecter les obligations d'information prévues à l'article 14, de manière spécifique et dans un délai déterminé ;

5° d'ordonner aux entités concernées d'informer les personnes physiques ou morales à l'égard desquelles elles fournissent des services ou exercent des activités susceptibles d'être affectées par une cybermenace importante de la nature de la menace, ainsi que de toutes mesures préventives ou réparatrices que ces personnes physiques ou morales pourraient prendre en réponse à cette menace ;

6° d'ordonner aux entités concernées de mettre en œuvre les recommandations formulées à la suite d'un audit de sécurité dans un délai raisonnable ;

7° d'ordonner aux entités concernées de rendre publics des aspects de violations de la présente loi de manière spécifique ;

8° d'imposer une amende administrative en vertu de l'article 26 en plus de l'une ou l'autre des mesures visées aux points 1° à 7°.

(5) L'article 22, paragraphes 6, 7 et 8, s'applique mutatis mutandis aux mesures de supervision et d'exécution prévues au présent article pour les entités importantes.

(6) Les autorités compétentes en vertu de la présente loi coopèrent avec les autorités compétentes pertinentes de l'État membre de l'Union européenne concerné au titre du règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) n° 1060/2009, (UE) n° 648/2012, (UE) n° 600/2014, (UE) n° 909/2014 et (UE) 2016/1011. Les autorités compétentes au titre de la présente loi informent le forum de supervision établi en vertu de l'article 32, paragraphe 1er, du règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) n° 1060/2009, (UE) n° 648/2012, (UE) n° 600/2014, (UE) n° 909/2014 et (UE) 2016/1011 lorsqu'elles exercent leurs pouvoirs de supervision et d'exécution dans le but de garantir qu'une entité importante qui a été désignée comme étant un prestataire tiers critique de services TIC en vertu de l'article 31 dudit règlement respecte la présente loi.

Art. 24. (1) Lorsque les autorités compétentes prennent connaissance, dans le cadre de la supervision ou de l'exécution, du fait que la violation commise par une entité essentielle ou importante à l'égard des obligations énoncées aux articles 12 et 14 peut donner lieu à une violation de données à caractère personnel au sens de l'article 4, point 12°, 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 abrogeant la directive 95/46/CE (règlement général sur la protection des données), tel que modifié, devant être notifiée en vertu de l'article 33 dudit règlement, elles en informent sans retard injustifié les autorités de contrôle visées à l'article 55 ou 56 dudit règlement.

(2) Lorsque les autorités de contrôle visées à l'article 55 ou 56 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 abrogeant la directive 95/46/CE (règlement général sur la protection des données), tel que modifié, imposent une amende administrative en vertu de l'article 58, paragraphe 2, point i), dudit règlement, les autorités compétentes n'imposent pas d'amende administrative au titre de l'article 26 pour une violation visée au paragraphe 1er et découlant du même comportement que celui qui a fait l'objet d'une amende administrative au titre de l'article 58, paragraphe 2, point i), 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 abrogeant la directive 95/46/CE (règlement général sur la protection des données), tel que modifié. Les autorités compétentes peuvent toutefois imposer les mesures d'exécution prévues à l'article 22, paragraphe 4, points 1° à 8°, à l'article 22, paragraphe 5, et à l'article 23, paragraphe 4, points 1° à 7°.

(3) Lorsque l'autorité de contrôle compétente 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 abrogeant la directive 95/46/CE (règlement général sur la protection des

données), tel que modifié, est établie dans un autre État membre de l'Union européenne que l'autorité compétente, l'autorité compétente informe l'autorité de contrôle luxembourgeoise de la violation potentielle de données à caractère personnel visée au paragraphe 1er.

Art. 25. (1) Lorsque l'autorité compétente concernée constate une violation des obligations prévues par les articles 11, paragraphe 4, 13, paragraphes 1er et 2, 15, 17, paragraphes 1er, alinéa 1er, et 2, et 18, paragraphes 1er à 6, elle peut frapper l'entité essentielle ou importante concernée d'une ou de plusieurs des sanctions suivantes :

1° un avertissement ;
2° un blâme ;
3° une amende administrative, 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 250 000 euros.

(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'entité essentielle ou importante concernée a la possibilité de consulter le dossier et de présenter ses observations. L'entité essentielle ou importante concernée peut se faire assister ou représenter par une personne de son choix. À l'issue de la procédure contradictoire, l'autorité compétente concernée peut prononcer à l'encontre de l'entité essentielle ou importante concernée 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'entité essentielle ou importante concernée.

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

(5) L'Administration de l'enregistrement, des domaines et de la TVA est chargée du recouvrement des amendes administratives qui lui sont communiquées par l'Institut luxembourgeois de régulation moyennant la transmission d'une copie des décisions de fixation. Le recouvrement est poursuivi comme en matière d'enregistrement.

Art. 26. (1) Les amendes administratives imposées aux entités essentielles et importantes pour des violations de la présente loi sont effectives, proportionnées et dissuasives, compte tenu des circonstances de chaque cas.

(2) Les amendes administratives sont imposées en complément de l'une ou l'autre des mesures visées à l'article 22, paragraphe 4, points 1° à 8°, à l'article 22, paragraphe 5, et à l'article 23, paragraphe 4, points 1° à 7°.

(3) Au moment de décider s'il y a lieu d'imposer une amende administrative et de décider de son montant, dans chaque cas d'espèce, il est dûment tenu compte, au minimum, des éléments prévus à l'article 22, paragraphe 7.

(4) Lorsqu'elles violent l'article 12 ou 14, paragraphes 1er à 4, les entités essentielles sont soumises, conformément aux paragraphes 2 et 3, à des amendes administratives d'un montant maximal s'élevant à 10 000 000 EUR ou à 2 % du chiffre d'affaires annuel mondial total de l'exercice précédent de l'entreprise à laquelle l'entité essentielle appartient, le montant le plus élevé étant retenu.

(5) Lorsqu'elles violent l'article 12 ou 14, paragraphes 1er à 4, les entités importantes sont soumises, conformément aux paragraphes 2 et 3, à des amendes administratives d'un

montant maximal s'élevant à 7 000 000 EUR ou à 1,4 % du chiffre d'affaires annuel mondial total de l'exercice précédent de l'entreprise à laquelle l'entité importante appartient, le montant le plus élevé étant retenu.

(6) Les amendes administratives prévues aux paragraphes 4 et 5 sont prononcées dans le respect de la procédure prévue à l'article 25, paragraphes 2 à 5.

(7) Les autorités compétentes ont le pouvoir d'assortir leur décision de sanction d'une astreinte pour contraindre une entité essentielle ou importante à mettre un terme à une violation de la présente loi.

Le montant de l'astreinte par jour à raison du manquement constaté ne peut être supérieur à 1 250 euros, sans que le montant total imposé à raison du manquement constaté ne puisse dépasser 25 000 euros.

Art. 27. (1) Lorsqu'une entité fournit des services dans plusieurs États membres de l'Union européenne, ou fournit des services dans un ou plusieurs États membres de l'Union européenne alors que ses réseaux et systèmes d'information sont situés dans un ou plusieurs autres États membres de l'Union européenne, les autorités compétentes des États membres de l'Union européenne concernés coopèrent et se prêtent mutuellement assistance si nécessaire. Cette coopération suppose, au minimum :

1° que les autorités compétentes appliquant des mesures de supervision ou d'exécution dans un État membre de l'Union européenne informent et consultent, par l'intermédiaire du point de contact unique, les autorités compétentes des autres États membres de l'Union européenne concernés en ce qui concerne les mesures de supervision et d'exécution prises ;

2° qu'une autorité compétente puisse demander à une autre autorité compétente de prendre des mesures de supervision ou d'exécution ;

3° qu'une autorité compétente, dès réception d'une demande motivée d'une autre autorité compétente, fournisse à l'autre autorité compétente une assistance mutuelle proportionnée à ses propres ressources afin que les mesures de supervision ou d'exécution puissent être mises en œuvre de manière effective, efficace et cohérente.

L'assistance mutuelle visée à l'alinéa 1er, point 3°, peut porter sur des demandes d'informations et des mesures de contrôle, y compris des demandes de procéder à des inspections sur place, à des contrôles à distance ou à des audits de sécurité ciblés. Une autorité compétente à laquelle une demande d'assistance est adressée ne peut refuser cette demande que s'il est établi que l'autorité n'est pas compétente pour fournir l'assistance demandée, que l'assistance demandée n'est pas proportionnée aux tâches de supervision de l'autorité compétente ou que la demande concerne des informations ou implique des activités dont la divulgation ou l'exercice seraient contraires aux intérêts essentiels de la sécurité nationale, la sécurité publique ou la défense de cet État membre de l'Union européenne. Avant de refuser une telle demande, l'autorité compétente consulte les autres autorités compétentes concernées ainsi que, à la demande de l'un des États membres de l'Union européenne concernés, la Commission européenne et l'ENISA.

(2) Le cas échéant et d'un commun accord, les autorités compétentes de différents États membres de l'Union européenne peuvent mener à bien des actions communes de supervision.

Chapitre 7 – Dispositions modificatives

Art. 28. À l'article 45*bis*, paragraphe 3, de la loi modifiée du 14 août 2000 relative au commerce électronique, les lettres a) et b) sont abrogées.

Art. 29. La loi modifiée du 23 juillet 2016 portant création d'un Haut-Commissariat à la Protection nationale est modifiée comme suit :

1° À l'article 2, le point 5° est remplacé comme suit :

« 5. « réseau et système d'information » : le réseau et système d'information au sens de l'article 2, point 1°, de la loi du XXXX concernant des mesures destinées à assurer un niveau élevé de cybersécurité ;

6. « cybersécurité » : la cybersécurité au sens de l'article 2, point 3°, de la loi du XXXX concernant des mesures destinées à assurer un niveau élevé de cybersécurité ;

7. « stratégie nationale en matière de cybersécurité » : un cadre cohérent fournissant des objectifs et des priorités stratégiques dans le domaine de la cybersécurité et de la gouvernance en vue de les réaliser au niveau national ;

8. « incident » : l'incident au sens de l'article 2, point 5°, de la loi du XXXX concernant des mesures destinées à assurer un niveau élevé de cybersécurité ;

9. « gestion des incidents » : gestion des incidents au sens de l'article 2, point 7°, de la loi du XXXX concernant des mesures destinées à assurer un niveau élevé de cybersécurité ;

10. « cybermenace » : la cybermenace au sens de l'article 2, point 9°, de la loi du XXXX concernant des mesures destinées à assurer un niveau élevé de cybersécurité ;

11. « vulnérabilité » : la vulnérabilité au sens de l'article 2, point 14°, de la loi du XXXX concernant des mesures destinées à assurer un niveau élevé de cybersécurité. » ;

2° L'article 3 est modifié comme suit :

a) au paragraphe 1er, lettre b), point 4°, les termes « stratégie nationale en matière de sécurité des réseaux et des systèmes d'information » sont remplacés par ceux de « stratégie nationale en matière de cybersécurité » ;

b) au paragraphe 1er, lettre c), après le point 1°, il est inséré un nouveau point 1*bis*°, libellé comme suit :

Commenté [JS3]: 1*bis*° ???

« 1*bis*. de coordonner la communication de crise en situation de crise ; »

c) au paragraphe 1er*bis*, la lettre b) est remplacée par la disposition suivante :

« b) attributions dans sa fonction de Centre gouvernemental de réponse aux incidents de sécurité informatique (CSIRT), ci-après « GOVCERT.LU ». » ;

d) au paragraphe 1er*bis*, la lettre c) est abrogée ;

e) le paragraphe 1er*quater* est remplacé par le libellé suivant :

« (1*quater*) Dans sa fonction de GOVCERT.LU, le Haut-Commissariat à la Protection nationale a pour missions :

a) de constituer le point de contact unique dédié à la gestion des incidents affectant les réseaux et systèmes d'information des administrations et services de l'État et des établissements publics ;

b) d'assurer un service de veille, de détection, d'alerte et de réaction aux cybermenaces et aux vulnérabilités affectant les réseaux et systèmes d'information des administrations et services de l'État et, à leur demande, des établissements publics ;

c) d'assurer la fonction de centre national de réponse aux incidents de sécurité informatique, dénommé « CSIRT National », en

1. opérant comme le point de contact officiel national pour les CSIRT nationaux et gouvernementaux étrangers ;
2. opérant comme le point de contact officiel national pour la collecte, l'analyse et la distribution d'informations relatives aux cybermenaces et incidents qui concernent les réseaux et systèmes d'information implantés au Grand-Duché de Luxembourg ;
3. relayant les informations collectées aux CSIRT sectoriels en charge de la cible d'une attaque ou, à défaut de CSIRT sectoriel, directement à la cible ;
4. assurant un service de veille aux cybermenaces et aux vulnérabilités et en réagissant aux incidents et en apportant une assistance aux entités critiques, le cas échéant.

d) d'assurer la fonction de centre militaire de réponse aux incidents de sécurité informatique, dénommé « MILCERT.LU », en

1. opérant comme le point de contact officiel national pour les CSIRT militaires étrangers ;
2. assurant, à partir du territoire du Grand-Duché de Luxembourg, un service de veille, de détection, d'alerte et de réaction aux cybermenaces, vulnérabilités et incidents affectant les réseaux et les systèmes d'information de l'armée ;
3. opérant, à partir du territoire du Grand-Duché de Luxembourg, une équipe d'intervention spécialisée capable de prendre en charge la réponse aux incidents liés à ces réseaux et systèmes d'information.

Le Haut-Commissaire à la Protection nationale peut, dans l'intérêt de l'exécution des missions du GOVCERT.LU, demander leur concours aux agents des administrations et services de l'État. »

f) le paragraphe 1er*quinquies* est abrogé.

3° Le chapitre 4*bis* est remplacé par la disposition suivante :

« **Chapitre 4*bis* – La stratégie nationale en matière de cybersécurité**

Art. 9*bis*. (1) Le Haut-Commissariat à la Protection nationale adopte une stratégie nationale en matière de cybersécurité qui détermine les objectifs stratégiques, les ressources nécessaires pour atteindre ces objectifs ainsi que les mesures politiques et

réglementaires appropriées, en vue de parvenir à un niveau élevé de cybersécurité et de le maintenir. La stratégie nationale en matière de cybersécurité comprend :

a) les objectifs et priorités de la stratégie en matière de cybersécurité, couvrant en particulier les secteurs visés aux annexes I et II de la loi du XXXX concernant des mesures destinées à assurer un niveau élevé de cybersécurité ;

b) un cadre de gouvernance visant à atteindre les objectifs et priorités visés à la lettre a) du présent paragraphe, y compris les politiques visées au paragraphe 2 ;

c) un cadre de gouvernance précisant les rôles et les responsabilités des parties prenantes concernées, et sur lequel reposent la coopération et la coordination entre les autorités compétentes, le point de contact unique et les CSIRT en vertu de la loi du XXXX concernant des mesures destinées à assurer un niveau élevé de cybersécurité, ainsi que la coordination et la coopération entre ces organismes et les autorités compétentes en vertu d'actes juridiques sectoriels de l'Union européenne ;

d) un mécanisme visant à déterminer les actifs pertinents et une évaluation des risques ;

e) un inventaire des mesures garantissant la préparation, la réaction et la récupération des services après incident, y compris la coopération entre les secteurs public et privé ;

f) une liste des différents acteurs et autorités concernés par la mise en œuvre de la stratégie nationale en matière de cybersécurité ;

g) un cadre politique visant une coordination renforcée entre les autorités compétentes en vertu de la présente loi et de la loi du XXX sur la résilience des entités critiques aux fins du partage d'informations relatives aux risques, aux menaces et aux incidents dans les domaines cyber et non cyber et de l'exercice des tâches de supervision, le cas échéant ;

h) un plan comprenant les mesures nécessaires en vue d'améliorer le niveau général de sensibilisation des citoyens à la cybersécurité.

(2) Dans le cadre de la stratégie nationale en matière de cybersécurité, le Haut-Commissariat à la Protection nationale adopte notamment des politiques portant sur les éléments suivants :

a) la cybersécurité dans le cadre de la chaîne d'approvisionnement des produits et services TIC utilisés par des entités pour la fourniture de leurs services ;

b) l'inclusion et la spécification d'exigences liées à la cybersécurité pour les produits et services TIC dans les marchés publics, y compris concernant la certification de cybersécurité, le chiffrement et l'utilisation de produits de cybersécurité en sources ouvertes ;

c) la gestion des vulnérabilités, y compris la promotion et la facilitation de la divulgation coordonnée des vulnérabilités en vertu de l'article 9, paragraphe 1er, de la loi du XXXX concernant des mesures destinées à assurer un niveau élevé de cybersécurité ;

d) le maintien de la disponibilité générale, de l'intégrité et de la confidentialité du noyau public de l'internet ouvert, y compris, le cas échéant, la cybersécurité des câbles de communication sous-marins ;

e) la promotion du développement et de l'intégration de technologies avancées pertinentes visant à mettre en œuvre des mesures de pointe dans la gestion des risques en matière de cybersécurité ;

f) la promotion et le développement de l'éducation et de la formation en matière de cybersécurité, des compétences en matière de cybersécurité, des initiatives de sensibilisation et de recherche et développement en matière de cybersécurité, ainsi que des orientations sur les bonnes pratiques de cyberhygiène et les contrôles, à l'intention des citoyens, des parties prenantes et des entités ;

g) le soutien aux institutions universitaires et de recherche visant à développer, améliorer et promouvoir le déploiement des outils de cybersécurité et à sécuriser les infrastructures de réseau ;

h) la mise en place de procédures pertinentes et d'outils de partage d'informations appropriés visant à soutenir le partage volontaire d'informations sur la cybersécurité entre les entités conformément au droit de l'Union européenne ;

i) le renforcement des valeurs de cyberrésilience et de cyberhygiène des petites et moyennes entreprises, en particulier celles qui sont exclues du champ d'application de la présente loi, en fournissant des orientations et un soutien facilement accessibles pour répondre à leurs besoins spécifiques ;

j) la promotion d'une cyberprotection active.

Le Haut-Commissariat à la Protection nationale évalue régulièrement la stratégie nationale en matière de cybersécurité, et au moins tous les cinq ans, sur la base d'indicateurs clés de performance et, le cas échéant, les modifient. » ;

4° Après l'article 9*bis,* il est inséré un nouveau chapitre 4*ter*, libellé comme suit :

« **Chapitre 4*ter* – Le plan national de réaction aux crises et incidents de cybersécurité majeurs**

Art. 9*ter.* Le Haut-Commissariat à la Protection nationale adopte un plan national de réaction aux crises et incidents de cybersécurité majeurs dans lequel sont définis les objectifs et les modalités de gestion des incidents de cybersécurité majeurs et des crises. Ce plan établit notamment les éléments suivants :

a) les objectifs des mesures et activités nationales de préparation ;

b) les tâches et responsabilités de l'autorité de gestion des crises cyber en vertu de la loi du XXXX concernant des mesures destinées à assurer un niveau élevé de cybersécurité ;

c) les procédures de gestion des crises cyber, y compris leur intégration dans le cadre national général de gestion des crises et les canaux d'échange d'informations ;

d) les mesures de préparation nationales, y compris des exercices et des activités de formation ;

e) les parties prenantes et les infrastructures des secteurs public et privé concernées ;

f) les procédures et arrangements nationaux entre les autorités et les organismes nationaux compétents visant à garantir la participation et le soutien effectifs à la gestion coordonnée des incidents de cybersécurité majeurs et des crises au niveau de l'Union européenne. » ;

5° A l'article 15*bis*, les termes « Le personnel de l'ANSSI, du CERT Gouvernemental et du SCC » sont remplacés par ceux de « Le personnel de l'ANSSI et du GOVCERT.LU ».

Art. 30. La loi du 28 mai 2019 portant transposition de la directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union européenne et modifiant 1° la loi modifiée du 20 avril 2009 portant création du Centre des technologies de l'information de l'État et 2° la loi du 23 juillet 2016 portant création d'un Haut-Commissariat à la Protection nationale est abrogée.

Art. 31. Les articles 42 et 43 de la loi du 17 décembre 2021 sur les réseaux et les services de communications électroniques sont abrogés.

Chapitre 8 – Intitulé de citation

Art. 32. La référence à la présente loi se fait sous la forme suivante : « loi du XXXX concernant des mesures destinées à assurer un niveau élevé de cybersécurité ».

ANNEXE I

Secteurs hautement critiques

Secteur	Sous-secteur	Type d'entité
1. Énergie	a) Électricité	- Entreprises d'électricité au sens de l'article 1er, point 14°, de la loi modifiée du 1er août 2007 relative à

		l'organisation du marché de l'électricité, qui remplissent la fonction de « fourniture » au sens de l'article 1er, point 21°, de ladite loi
		- Gestionnaires de réseau de distribution au sens de l'article 1er, point 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, point 25°, de la loi modifiée du 1er août 2007 relative à l'organisation du marché de l'électricité
		- Producteurs au sens de l'article 1er, point 39°, de la loi modifiée du 1er août 2007 relative à l'organisation du marché de l'électricité
		- Opérateurs désignés du marché de l'électricité au sens de l'article 2, point 8°, du règlement (UE) 2019/943 du Parlement européen et du Conseil du 5 juin 2019 sur le marché intérieur de l'électricité, tel que modifié - Acteurs du marché au sens de l'article 2, point 25°, du règlement (UE) 2019/943 du Parlement européen et du Conseil du 5 juin 2019 sur le marché intérieur de l'électricité, tel que modifié, fournissant des services d'agrégation, de participation active de la demande ou de stockage d'énergie au sens de l'article 1er, points 1*quindecies°*, 31*quater°* et 49*ter°*, de la loi modifiée du 1er août 2007 relative à l'organisation du marché de l'électricité - Exploitants d'un point de recharge qui sont responsables de la gestion et de l'exploitation d'un point de recharge, lequel fournit un service de recharge aux utilisateurs finals, y compris au nom et pour le compte d'un prestataire de services de mobilité
	b) Réseaux de chaleur et de froid	- Opérateurs de réseaux de chaleur ou de réseaux de froid au sens de l'article 2, point 19°, de la directive (UE) 2018/2001 du Parlement européen et du Conseil du 11 décembre 2018 relative à la promotion de l'utilisation de l'énergie produite à partir de sources renouvelables
	c) Pétrole	- Exploitants d'oléoducs

		- Exploitants d'installations de production, de raffinage, de traitement, de stockage et de transport de pétrole
		- Entités centrales de stockage au sens de l'article 1er, lettre g), de la loi modifiée du 10 février 2015 relative à l'organisation du marché de produits pétroliers
	d) Gaz	- Entreprises de fourniture au sens de l'article 1er, point 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, point 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, point 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, point 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, point 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, point 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
	e) Hydrogène	- Exploitants de systèmes de production, de stockage et de transport d'hydrogène
2. Transports	a) Transports aériens	- Transporteurs aériens au sens de l'article 3, point 4°, du règlement (CE) no 300/2008 du Parlement européen et du Conseil du 11 mars 2008 relatif à l'instauration de règles communes dans le domaine de la sûreté de l'aviation civile et abrogeant le règlement (CE) n°2320/2002, tel que modifié, utilisés à des fins commerciales

		- Entités gestionnaires d'aéroports au sens de l'article 2, point 1°, de la loi modifiée 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 au sens de l'article 2, point 1°, de la directive 2009/12/CE du Parlement européen et du Conseil du 11 mars 2009 sur les redevances aéroportuaires, y compris les aéroports du réseau central énumérés à l'annexe II, section 2, du règlement (UE) n°1315/2013 du Parlement européen et du Conseil du 11 décembre 2013 sur les orientations de l'Union pour le développement du réseau transeuropéen de transport et abrogeant la décision n°661/2010/UE, tel que modifié, 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 »), tel que modifié
	b) Transports ferroviaires	- Gestionnaires de l'infrastructure au sens de l'article 2, point 31°, de la loi du 5 février 2021 relative à l'interopérabilité ferroviaire, à la sécurité ferroviaire et à la certification des conducteurs de train
		- Entreprises ferroviaires au sens de l'article 2, point 15°, de la loi modifiée du 6 juin 2019 portant transposition de la directive (UE) 2016/2370 du Parlement européen et du Conseil du

		14 décembre 2016 modifiant la directive 2012/34/UE en ce qui concerne l'ouverture du marché des services nationaux de transport de voyageurs par chemin de fer et la gouvernance de l'infrastructure ferroviaire, y compris les exploitants d'installation de service au sens de l'article 2, point 18°, de la même loi
	c) Transports par eau	- Sociétés de transport par voie d'eau intérieure, maritime et côtier de passagers et de fret, telles qu'elles sont définies pour le domaine du transport maritime à 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, tel que modifié, 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 du Parlement européen et du Conseil du 31 mars 2004 relatif à l'amélioration de la sûreté des navires et des installations portuaires, tel que modifié, ainsi que les entités exploitant des infrastructures et des équipements à l'intérieur des ports
		- Exploitants de services de trafic maritime (STM) 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) Transports routiers	- 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 la gestion de la circulation, à l'exclusion des entités publiques pour lesquelles la gestion de la circulation ou l'exploitation de systèmes de transport intelligents constituent une partie non essentielle de leur activité générale
		- 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. Secteur bancaire		Établissements de crédit au sens de l'article 4, point 1°, du règlement (UE) n°575/2013 du Parlement européen et du Conseil du 26 juin 2013 concernant les exigences prudentielles applicables aux établissements de crédit et aux entreprises d'investissement et modifiant le règlement (UE) n°648/2012, tel que modifié
4. Infrastructures des marchés financiers		- Exploitants de plates-formes de négociation au sens de l'article 1er, point 43°, de la loi modifiée 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, tel que modifié
5. Santé		- Prestataires de soins de santé au sens de l'article 2, lettre e), de la loi modifiée du 24 juillet 2014 relative aux droits et obligations du patient
		- Laboratoires de référence de l'Union européenne visés à l'article 15 du règlement (UE) 2022/2371 du Parlement européen et du Conseil du 23 novembre 2022 concernant les menaces transfrontières graves pour la santé et abrogeant la décision n°1082/2013/UE
		- Laboratoires nationaux de référence désignés en vertu de l'article 10 de la loi modifiée du 1er août 2018 sur la

		déclaration obligatoire de certaines maladies dans le cadre de la protection de la santé publique
		- Entités exerçant des activités de recherche et de développement dans le domaine des médicaments au sens de l'article 1er, point 2°, de la directive 2001/83/CE du Parlement européen et du Conseil du 6 novembre 2001 instituant un code communautaire relatif aux médicaments à usage humain - Entités fabriquant des produits pharmaceutiques de base et des préparations pharmaceutiques au sens de la NACE Rév. 2 Nomenclature statistique des activités économiques dans la Communauté européenne, section C, division 21 - Entités fabriquant des dispositifs médicaux considérés comme critiques en cas d'urgence de santé publique (liste des dispositifs médicaux critiques en cas d'urgence de santé publique) au sens de l'article 22 du règlement (UE) 2022/123 du Parlement européen et du Conseil du 25 janvier 2022 relatif à un rôle renforcé de l'Agence européenne des médicaments dans la préparation aux crises et la gestion de celles-ci en ce qui concerne les médicaments et les dispositifs médicaux, tel que modifié
6. Eau potable		Fournisseurs et distributeurs d'eaux destinées à la consommation humaine au sens de l'article 2, point 1°, lettre a), de la loi du 23 décembre 2022 relative à la qualité des eaux destinées à la consommation humaine et modifiant la loi modifiée du 19 décembre 2008 relative à l'eau, à l'exclusion des distributeurs pour lesquels la distribution d'eaux destinées à la consommation humaine constitue une partie non essentielle de leur activité générale de distribution d'autres produits et biens
7. Eaux usées		Entreprises collectant, évacuant ou traitant les eaux urbaines résiduaires, les eaux ménagères usées ou les eaux industrielles usées au sens de l'article 2, points 1°, 2° et 3°, du règlement grand-ducal modifié du 13 mai 1994 relatif au traitement des eaux urbaines résiduaires, à l'exclusion des entreprises pour

		lesquelles la collecte, l'évacuation ou le traitement des eaux urbaines résiduaires, des eaux ménagères usées ou des eaux industrielles usées constituent une partie non essentielle de leur activité générale
8. Infrastructure numérique		- Fournisseurs de points d'échange internet
		- Fournisseurs de services DNS, à l'exclusion des opérateurs de serveurs racines de noms de domaine
		- Registres de noms de domaine de premier niveau
		- Fournisseurs de services d'informatique en nuage
		- Fournisseurs de services de centres de données
		- Fournisseurs de réseaux de diffusion de contenu
		- Prestataires de services de confiance
		- Fournisseurs de réseaux de communications électroniques publics
		- Fournisseurs de services de communications électroniques accessibles au public
9. Gestion des services TIC (interentreprises)		- Fournisseurs de services gérés - Fournisseurs de services de sécurité gérés
10. Administration publique		Entités de l'administration publique telle que définie à l'article 2, point 34°
11. Espace		Exploitants d'infrastructures terrestres, détenues, gérées et exploitées par des États membres de l'Union européenne ou par des parties privées, qui soutiennent la fourniture de services spatiaux, à l'exclusion des fournisseurs de réseaux de communications électroniques publics

ANNEXE II

Autres secteurs critiques

Secteur	Sous-secteur	Type d'entité
1. Services postaux et d'expédition		Prestataires de services postaux au sens de l'article 1er, point 12°, de la loi modifiée du 26 décembre 2012 sur les services postaux, y compris les prestataires de services d'expédition
2. Gestion des déchets		Entreprises exécutant des opérations de gestion des déchets au sens de l'article 4, point 22°, de la loi modifiée du 21 mars 2012 relative aux déchets, à l'exclusion des entreprises pour lesquelles la gestion des déchets n'est pas la principale activité économique
3. Fabrication, production et distribution de produits chimiques		Entreprises procédant à la fabrication de substances et à la distribution de substances ou de mélanges au sens de l'article 3, points 9° et 14°, du règlement (CE) n°1907/2006 du Parlement européen et du Conseil du 18 décembre 2006 concernant l'enregistrement, l'évaluation et l'autorisation des substances chimiques, ainsi que les restrictions applicables à ces substances (REACH), instituant une agence européenne des produits chimiques, modifiant la directive 1999/45/CE et abrogeant le règlement (CEE) n°793/93 du Conseil et le règlement (CE) n°1488/94 de la Commission ainsi que la directive 76/769/CEE du Conseil et les directives 91/155/CEE, 93/67/CEE, 93/105/CE et 2000/21/CE de la Commission, tel que modifié, et entreprises procédant à la production d'articles au sens de l'article 3, point 3°, dudit règlement, à partir de substances ou de mélanges
4. Production, transformation et distribution des denrées alimentaires		Entreprises du secteur alimentaire au sens de l'article 3, point 2°, du règlement (CE) n°178/2002 du Parlement européen et du Conseil du 28 janvier 2002 établissant les principes généraux et les prescriptions générales de la législation alimentaire, instituant l'Autorité européenne de sécurité des aliments et fixant des procédures relatives à la sécurité des denrées alimentaires, tel que modifié, qui exercent des activités de distribution en gros ainsi que de

		production et de transformation industrielles
5. Fabrication	a) Fabrication de dispositifs médicaux et de dispositifs médicaux de diagnostic in vitro	Entités fabriquant des dispositifs médicaux au sens de l'article 2, point 1°, du règlement (UE) 2017/745 du Parlement européen et du Conseil du 5 avril 2017 relatif aux dispositifs médicaux, modifiant la directive 2001/83/CE, le règlement (CE) n°178/2002 et le règlement (CE) n°1223/2009 et abrogeant les directives du Conseil 90/385/CEE et 93/42/CEE, tel que modifié, et entités fabriquant des dispositifs médicaux de diagnostic in vitro au sens de l'article 2, point 2°, du règlement (UE) 2017/746 du Parlement européen et du Conseil du 5 avril 2017 relatif aux dispositifs médicaux de diagnostic in vitro et abrogeant la directive 98/79/CE et la décision 2010/227/UE de la Commission, tel que modifié, à l'exception des entités fabriquant des dispositifs médicaux mentionnés à l'annexe I, point 5°, cinquième tiret
	b) Fabrication de produits informatiques, électroniques et optiques	Entreprises exerçant l'une des activités économiques visées dans la NACE Rév. 2 Nomenclature statistique des activités économiques dans la Communauté européenne, section C, division 26
	c) Fabrication d'équipements électriques	Entreprises exerçant l'une des activités économiques visées dans la NACE Rév. 2 Nomenclature statistique des activités économiques dans la Communauté européenne, section C, division 27
	d) Fabrication de machines et équipements n.c.a.	Entreprises exerçant l'une des activités économiques visées dans la NACE Rév. 2 Nomenclature statistique des activités économiques dans la Communauté européenne, section C, division 28
	e) Construction de véhicules automobiles, remorques et semi-remorques	Entreprises exerçant l'une des activités économiques visées dans la NACE Rév. 2 Nomenclature statistique des activités économiques dans la Communauté européenne, section C, division 29
	f) Fabrication d'autres matériels de transport	Entreprises exerçant l'une des activités économiques visées dans la NACE Rév. 2 Nomenclature statistique des activités économiques dans la Communauté européenne, section C, division 30
6. Fournisseurs numériques		- Fournisseurs de places de marché en ligne
		- Fournisseurs de moteurs de recherche en ligne

		- Fournisseurs de plateformes de services de réseaux sociaux
7. Recherche		Organismes de recherche

Luxembourg, le 13 avril 2026

Le Président-Rapporteur
Laurent Zeimet