N° 8307

CHAMBRE DES DEPUTES

PROJET DE LOI

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

* * *

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

Le projet de loi n° 8307 a été déposé à la Chambre des Députés le 1er septembre 2023 par Monsieur Xavier Bettel, Premier ministre, Ministre d'Etat.

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

En date du 2 octobre 2023, le projet de loi a été renvoyé à la Commission des Institutions (ci-après la « Commission »).

La Chambre des Fonctionnaires et Employés publics (CHFEP) a émis son avis le 25 octobre 2023.

En date du 7 décembre 2023, la Chambre de Commerce a émis son avis.

L'avis du Conseil d'État date du 23 janvier 2024.

Le 9 février 2024, la Commission a désigné M. Laurent Zeimet comme rapporteur du projet de loi.

Le 13 mars 2024, la Commission s'est vu présenter le projet de loi et a examiné les avis de la CHFEP, de la Chambre de Commerce et du Conseil d'Etat.

Le 23 avril 2025, la Commission nationale pour la protection des données (CNPD) a rendu son avis.

Le 29 janvier et le 13 mai 2025, le projet de loi a fait l'objet d'une série d'amendements gouvernementaux avisés par le Conseil d'Etat dans son avis complémentaire du 13 mai 2025.

Lors de sa réunion du 10 novembre 2025, la Commission a adopté une série d'amendements parlementaires.

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

Lors de sa réunion du 9 février 2026, la Commission a examiné l'avis précité et a adopté une série d'amendements parlementaires.

Le 10 mars 2026, le Conseil d'Etat a émis son troisième 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 projet de loi n° 8307 a pour objet la 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 (Critical Entities Resilience Directive, ci-après « directive CER »), afin d'établir un cadre national cohérent pour le recensement, la désignation et la supervision des entités critiques fournissant des services essentiels au maintien de fonctions sociétales ou d'activités économiques vitales au Grand-Duché de Luxembourg.

À cette fin, le projet de loi prévoit notamment la mise en place d'une stratégie nationale en matière de résilience ainsi que la réalisation d'une évaluation des risques au niveau national, sur la base desquelles les entités critiques sont identifiées.

Il instaure en outre un ensemble d'obligations à charge des entités critiques, comprenant l'évaluation périodique des risques susceptibles de perturber la fourniture de leurs services essentiels, la mise en place de mesures techniques, de sécurité et organisationnelles appropriées et proportionnées pour garantir leur résilience, la notification des incidents significatifs aux autorités compétentes, ainsi que la possibilité de procéder à des vérifications des antécédents des personnes occupant des fonctions sensibles, dans le respect des procédures prévues.

III. Considérations générales

Le projet de loi n° 8307 s'inscrit dans le cadre de la transposition de la directive (UE) 2022/2557 relative à la résilience des entités critiques, laquelle vise à renforcer la capacité des États membres à prévenir, résister et réagir aux perturbations affectant la fourniture de services essentiels.

À cette fin, le projet de loi met en place un cadre national visant à assurer un niveau élevé de résilience des entités critiques, entendues comme les entités publiques ou privées fournissant des services essentiels indispensables au maintien de fonctions sociétales vitales ou d'activités économiques essentielles.

Le dispositif repose sur une approche structurée, articulée autour de l'élaboration d'une stratégie nationale en matière de résilience, de la réalisation d'une évaluation des risques au niveau national ainsi que du recensement et de la désignation des entités critiques.

À cet égard, le Haut-Commissariat à la Protection nationale (HCPN) est chargé de définir les objectifs stratégiques, les priorités ainsi que les mesures à mettre en œuvre, tout en assurant la coordination entre les différents acteurs concernés. Il procède également à une évaluation des risques, tenant compte notamment des risques naturels et d'origine humaine, des interdépendances sectorielles et transfrontalières ainsi que des informations relatives aux incidents. Cette évaluation constitue un élément central du dispositif, en ce qu'elle permet d'identifier les entités critiques et de soutenir celles-ci dans la mise en œuvre des mesures de résilience.

Sur cette base, les autorités compétentes procèdent au recensement et à la désignation des entités critiques dans les secteurs énumérés à l'annexe du projet de loi, tels que l'énergie, les transports, le secteur bancaire, les infrastructures des marchés financiers, la santé, l'eau, les infrastructures numériques ou encore l'administration publique. La désignation repose notamment sur l'importance des services fournis, l'impact potentiel d'un incident sur la société et l'économie ainsi que les interdépendances existantes entre secteurs.

Les entités ainsi désignées sont soumises à un ensemble d'obligations destinées à garantir leur résilience. Elles doivent notamment procéder à des évaluations régulières des risques, mettre en œuvre des mesures techniques, organisationnelles et de sécurité appropriées, établir des plans de résilience et notifier aux autorités compétentes les incidents significatifs affectant la continuité de leurs services.

Le projet de loi introduit en outre des dispositions spécifiques relatives à la sécurité du personnel, en prévoyant la possibilité de procéder à des vérifications des antécédents pour les personnes occupant des fonctions sensibles, selon une procédure encadrée impliquant notamment la Police grand-ducale et le ministre ayant la Protection nationale dans ses attributions.

Sur le plan institutionnel, le projet de loi désigne la Commission de surveillance du secteur financier (CSSF) et le Haut-Commissariat à la Protection nationale comme autorités compétentes, en fonction des secteurs concernés, et confie au HCPN le rôle de point de contact national unique chargé d'assurer la coopération au niveau européen et international.

Le dispositif prévoit également des mécanismes de supervision et d'exécution permettant aux autorités compétentes de contrôler le respect des obligations imposées aux entités critiques, notamment à travers des inspections, des audits et, le cas échéant, des injonctions. En cas

de manquement, des sanctions administratives peuvent être prononcées, allant de l'avertissement à l'amende administrative dont le montant maximal est fixé à 250 000 euros.

Le projet de loi prévoit par ailleurs certaines exclusions du champ d'application, notamment en ce qui concerne les entités relevant des domaines de la défense et de la sécurité nationale, telles que le Service de renseignement de l'État, la Direction de la défense et l'Armée luxembourgeoise, afin de tenir compte des spécificités de ces domaines et des exigences de confidentialité qui s'y attachent.

Par ailleurs, le projet de loi s'inscrit dans une logique de complémentarité avec le cadre européen en matière de cybersécurité, notamment la directive (UE) 2022/2555 (NIS 2) avec laquelle il entretient des liens étroits, en particulier en ce qui concerne la gestion des risques et la coopération entre autorités compétentes.

Enfin, le projet de loi procède à la modification de la loi modifiée du 23 juillet 2016 portant création d'un Haut-Commissariat à la Protection nationale, afin d'adapter les missions et les compétences de cette autorité aux nouvelles exigences découlant de la directive CER.

IV. Avis

a) Avis du Conseil d'État

a. Avis du 23 janvier 2024

Dans son avis du 23 janvier 2024, le Conseil d'État relève que le projet de loi a pour objectif principal la transposition de la directive (UE) 2022/2557 et marque son accord de principe avec l'approche retenue par les auteurs, consistant à procéder par une loi spéciale distincte de la loi modifiée du 23 juillet 2016 portant création du Haut-Commissariat à la Protection nationale. Il estime que ce choix se justifie notamment au regard du partage des compétences entre le HCPN et la Commission de surveillance du secteur financier.

La Haute Corporation émet plusieurs oppositions formelles.

D'abord, elle s'oppose à l'article 1er, paragraphe 2, relatif à l'articulation entre le régime national et les actes sectoriels de l'Union européenne. Elle estime que le texte, en l'absence d'un mécanisme de reconnaissance officielle de l'équivalence par l'État, laisse aux entités critiques le soin d'apprécier elles-mêmes si les obligations prévues par un acte sectoriel de l'Union européenne se substituent à celles prévues par la loi en projet, ce qui est jugé source d'insécurité juridique.

Ensuite, elle formule plusieurs oppositions formelles à l'égard du dispositif de vérification des antécédents prévu aux articles 13 à 15.

Elle s'oppose, en premier lieu, à la disposition selon laquelle les catégories de personnes soumises à une vérification des antécédents doivent faire l'objet d'un « avis favorable » de l'autorité compétente avant l'introduction même d'une demande individuelle. La Haute Corporation considère que le texte ne permet pas de déterminer avec suffisamment de clarté la nature de cette intervention, qui pourrait être comprise soit comme une approbation préalable de chaque proposition formulée par une entité critique, soit comme un acte à portée générale définissant les catégories de personnel concernées, cette ambiguïté étant source d'insécurité juridique.

Elle s'oppose, en deuxième lieu, à la disposition permettant à la Police grand-ducale d'accéder, sur la base d'une autorisation de la personne concernée, à « toute information relative à la demande disponible et directement accessible aux autorités compétentes nationales, ou tout document équivalent » auprès des autorités des pays de résidence ou de nationalité. Elle estime qu'une telle formulation ouvre, dans une matière réservée à la loi, l'accès à un ensemble indéterminé d'informations dont les contours ne sont pas définis avec la précision requise.

Une opposition formelle vise également le dispositif dans son ensemble, au motif qu'il manque de précision tant quant au déroulement de la procédure de vérification des antécédents que quant à l'autorité appelée à prendre la décision à son issue. Le Conseil d'État relève en particulier que le texte reste muet sur les suites à réserver à l'avis de la Police grand-ducale et qu'il entretient une confusion entre la procédure et son résultat. Il considère en outre que le dispositif ne prévoit pas de garanties suffisantes pour les personnes concernées, dès lors qu'il ne leur assure ni un accès adéquat au dossier ni des voies de recours effectives, et en conclut que le dispositif est contraire au principe de sécurité juridique ainsi qu'aux principes constitutionnels d'accès au juge et de recours effectif.

Une opposition formelle vise aussi l'article 19 relatif au régime des sanctions administratives. La Haute Corporation estime que le texte ne satisfait pas aux exigences du principe de légalité des peines et de spécification de l'incrimination, dans la mesure où il se borne à renvoyer globalement à certains articles du projet de loi, sans préciser les obligations exactes dont le non-respect est susceptible d'être sanctionné.

Enfin, le Conseil d'État émet plusieurs réserves. Il réserve sa position quant à la dispense du second vote constitutionnel en ce qui concerne l'article 14, s'interrogeant sur la pertinence et la proportionnalité du recours au casier judiciaire dans le cadre de la vérification de l'identité des personnes concernées, et maintient cette réserve en l'absence d'explications complémentaires des auteurs. Il émet également une réserve quant à la durée de conservation d'un an des données à caractère personnel prévue à l'article 15, paragraphe 2, qu'il juge insuffisamment justifiée au regard du principe de minimisation des données consacré par le RGPD. Il soulève enfin une difficulté au regard du principe d'égalité de traitement concernant la limitation de l'octroi de la prime d'astreinte aux seuls agents du Centre national de crise prévue à l'article 20.

Le Conseil d'État formule en outre plusieurs observations d'ordre légistique visant à harmoniser les intitulés des textes cités et à redresser certaines erreurs matérielles de renvoi et de numérotation.

b. Avis complémentaire du 13 mai 2025

Dans son avis complémentaire du 13 mai 2025, le Conseil d'État constate que les amendements gouvernementaux apportent des réponses substantielles aux observations formulées dans son avis du 23 janvier 2024 et reprennent, dans une large mesure, les propositions de texte ainsi que les recommandations d'ordre légistique qu'il avait émises. Il lève en conséquence plusieurs oppositions formelles formulées à l'encontre du projet de loi initial, relevant notamment que le nouveau dispositif prévu à l'article 14 organise désormais un processus décisionnel détaillé à la suite de l'avis de la Police grand-ducale et prévoit des voies de recours effectives.

La Haute Corporation maintient toutefois plusieurs oppositions formelles.

D'abord, elle s'oppose au libellé de l'article 13, paragraphe 4, alinéa 2, tel qu'amendé, en ce qu'il qualifie la vérification des antécédents d'« échouée ». Elle estime que cette terminologie est insuffisamment précise, dès lors que le texte ne permet ni de cerner la portée exacte d'un tel échec ni d'en déduire clairement les conséquences. Elle demande, sous peine d'opposition formelle pour insécurité juridique, que la disposition soit reformulée afin de prévoir explicitement que, lorsque la personne concernée relève de l'un des cas de figure visés, elle est considérée d'office comme présentant un risque pour la sécurité de l'entité critique, ce qui clôture la procédure devant la Police grand-ducale et appelle une décision du ministre.

Ensuite, elle réitère son opposition formelle pour insécurité juridique à l'endroit de l'article 14, paragraphe 4, alinéa 1er, en raison de la référence à la personne « qui a échoué à la vérification des antécédents », reprenant ainsi une terminologie dont elle a déjà relevé le caractère imprécis à l'article 13. Elle demande que la disposition vise plutôt la personne au sujet de laquelle le ministre a constaté, par sa décision, qu'elle constitue un risque potentiel pour la sécurité de l'entité critique.

Enfin, le Conseil d'État s'oppose à l'article 15, paragraphe 3, nouveau, en ce qu'il permet à la Police grand-ducale de conserver, pendant cinq ans à compter de l'effacement des données principales, un nombre limité de données à caractère personnel liées à la vérification des antécédents. Il rappelle que, conformément au principe de limitation de la conservation consacré par le RGPD, de telles données ne peuvent être conservées au-delà de la durée nécessaire au regard des finalités poursuivies, et demande, sous peine d'opposition formelle, que le texte précise qu'il s'agit d'un délai maximal de cinq ans.

Le Conseil d'État formule en outre plusieurs observations d'ordre légistique visant à harmoniser la rédaction des dispositions amendées et à assurer la cohérence des références au sein du texte.

c. Deuxième avis complémentaire du 8 décembre 2025

Dans son deuxième avis complémentaire du 8 décembre 2025, le Conseil d'État examine un amendement gouvernemental ainsi que les amendements parlementaires adoptés par la Commission des Institutions le 11 novembre 2025. Il constate que ces derniers visent à répondre aux oppositions formelles formulées dans son avis complémentaire du 13 mai 2025 et permettent, dans une large mesure, d'y donner suite.

La Haute Corporation lève ainsi l'opposition formelle relative à l'article 15, paragraphe 3, la Commission ayant complété la disposition par la mention d'un délai « maximal » de conservation des données. Elle lève également les oppositions formelles visant les articles 13 et 14, les reformulations proposées étant conformes à ses observations. Les autres amendements n'appellent pas d'observations de sa part.

Elle émet toutefois une opposition formelle à l'encontre de l'amendement gouvernemental modifiant l'article 8, en ce qu'il prévoit d'exclure du champ d'application de la loi certaines entités de l'administration publique exerçant des activités dans les domaines de la sécurité nationale. Sans contester le principe d'une telle exclusion, prévu par la directive (UE) 2022/2557, le Conseil d'État estime que la formulation retenue est source d'insécurité juridique, dès lors qu'elle ne désigne pas avec suffisamment de précision les entités concernées. Il préconise en conséquence de procéder à une désignation nominative des entités visées.

d. Troisième avis complémentaire du 10 mars 2026

Par dépêche du 10 février 2026, une série d'amendements parlementaires adoptés par la Commission des Institutions lors de sa réunion du 9 février 2026 a été transmise au Conseil d'État. Ces amendements ont pour objet de répondre à l'opposition formelle qu'il avait exprimée dans son avis complémentaire du 13 mai 2025, puis maintenue dans son deuxième avis complémentaire du 8 décembre 2025, concernant l'article 8 du projet de loi relatif au champ d'application.

À la lumière des modifications proposées, consistant à désigner nommément les entités concernées par l'exclusion du champ d'application, la Haute Corporation considère que l'opposition formelle peut être levée.

La Haute Corporation se limite, par ailleurs, à formuler quelques observations d'ordre légistique mineures. Les autres amendements n'appellent pas d'observations de sa part.

b) Avis de la Chambre des Fonctionnaires et Employés publics du 25 octobre 2023

Dans son avis du 25 octobre 2023, la Chambre des fonctionnaires et employés publics (CHFEP) constate que le projet de loi vise principalement à assurer la transposition de la directive (UE) 2022/2557 en droit national et n'émet pas d'observations particulières sur les dispositions de fond.

Elle formule toutefois des réserves à l'égard de l'article 20 du projet de loi initial, qui limitait l'octroi de la prime d'astreinte aux seuls agents chargés d'assurer l'opérationnalité permanente du Centre national de crise, estimant qu'une telle restriction n'est ni nécessaire ni justifiée au regard du cadre légal existant. La CHFEP demande dès lors le maintien du dispositif actuel sans modification. Cette réserve est finalement devenue sans objet à la suite de la suppression de l'article 20 par amendement gouvernemental.

c) Avis de la Chambre du Commerce du 7 décembre 2023

Dans son avis du 7 décembre 2023, la Chambre de Commerce accueille favorablement le projet de loi, dont elle souligne qu'il vise à assurer la transposition en droit national de la directive (UE) 2022/2557 relative à la résilience des entités critiques. Elle marque son accord avec l'approche retenue par les auteurs et avec les objectifs poursuivis en matière de renforcement de la résilience des services essentiels.

La Chambre de Commerce indique ne pas avoir d'observations particulières quant au fond du projet de loi et se limite à formuler une remarque d'ordre légistique.

d) Avis de la Commission nationale pour la protection des données du 23 avril 2025

Dans son avis du 23 avril 2025, la Commission nationale pour la protection des données (CNPD) tient compte des amendements gouvernementaux du 29 janvier 2025 et concentre son analyse sur les dispositions relatives à la vérification des antécédents. Elle se rallie globalement aux observations du Conseil d'État concernant les articles 13 à 15 et souligne que la base juridique de la vérification doit reposer sur l'obligation légale, plutôt que sur le consentement de la personne concernée. Elle invite également à mieux préciser les bases de données policières susceptibles d'être consultées.

La CNPD accueille favorablement plusieurs améliorations du texte. Elle salue notamment la précision des critères d'évaluation du risque à l'article 13, paragraphe 4, ainsi que la transmission d'un avis motivé par la Police grand-ducale au ministre compétent. Elle approuve aussi l'article 14, paragraphe 3, qui garantit que les données à caractère personnel ne sont pas transmises à l'entité requérante, tout en recommandant d'aligner la terminologie employée sur celle du RGPD.

Enfin, la CNPD se félicite de la durée de conservation des données limitée à six mois prévue à l'article 15, paragraphe 2, qu'elle juge conforme au principe de minimisation des données, et suggère d'envisager l'intégration de dispositions spécifiques relatives au secret de l'instruction, afin de renforcer encore la sécurité juridique.

V. Commentaire des articles

Ad article 1er

L'article 1er définit le champ d'application. Vu l'étroite relation entre le présent projet et 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,[1] ci-après « directive NIS 2 », il convient de veiller à ce que le champ d'application de chacun des deux textes soit clairement délimité. Ainsi, le paragraphe 1er dispose que la loi sous projet ne s'applique pas aux questions couvertes par la directive NIS 2, qui impose aux entités essentielles et importantes des exigences en matière de cybersécurité.

Le paragraphe 2 prévoit que lorsque des dispositions d'actes juridiques sectoriels de l'Union européenne exigent des entités critiques qu'elles prennent des mesures pour renforcer leur résilience, et lorsque ces exigences ont un effet au moins équivalent aux obligations correspondantes prévues par la présente loi, les dispositions pertinentes de la présente loi 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.[2]

Remarquons que la terminologie utilisée à l'article 1er, paragraphe 2, 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, ci-après « directive CER », a été légèrement adaptée dans le texte de transposition. En effet, il a été opté, dans un souci de cohérence, pour la terminologie « ont un effet au moins équivalent » reprise de la loi du 28 mai 2019 portant transposition 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.[3]

Ad article 2

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

[1] *J.O.U.E.*, L 333 du 27 décembre 2022, p. 80.

[2] Consid. (10), 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, ci-après « directive CER ».

[3] 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.

La définition sous l'article 2, point 1, définit l'« entité critique », qui a une fonction-clé dans le maintien de fonctions sociétales ou d'activités économiques vitales et qui constitue dès lors l'acteur principal de la directive CER. Une entité critique est une entité publique ou privée :

- appartenant à l'une des catégories qui figurent dans la troisième colonne du tableau de l'annexe,
- fournissant un ou plusieurs services essentiels,
- exerçant ses activités sur le territoire luxembourgeois et son infrastructure critique est située sur ledit territoire, et
- dont un incident aurait des effets perturbateurs importants sur la fourniture par l'entité d'un ou de plusieurs services essentiels ou sur la fourniture d'autres services essentiels dans les secteurs figurant à l'annexe qui dépendent dudit ou desdits services essentiels.

Alors que la directive 2008/114/CE[4] plaçait « l'infrastructure critique » au centre de la directive, la directive CER procède à un changement de paradigme en faisant de « l'entité critique » l'acteur principal de la directive. Ainsi, au lieu d'augmenter la résilience de l'infrastructure critique, qui vise essentiellement l'installation ou l'équipement, cette nouvelle directive veut que l'entité qui exploite cette infrastructure dispose des moyens nécessaires afin de pouvoir faire face aux risques qui pourraient porter préjudice à la fourniture des services essentiels.[5]

Le point 2° définit la « résilience ». La résilience des entités critiques est mise au cœur de la directive CER. Les entités critiques doivent être capables de prévenir tout incident qui pourrait perturber la fourniture de leurs services, de s'en protéger, d'y réagir, d'y résister, de l'atténuer, de l'absorber, de s'y adapter et de s'en rétablir, en adoptant une approche basée sur les risques. Tous les risques doivent être pris en compte, notamment les risques naturels, d'origine humaine, y compris ceux qui revêtent un caractère transsectoriel ou transfrontière, les accidents, les catastrophes naturelles, les urgences de santé publique, les menaces hybrides ou encore les menaces terroristes.

Un « incident », défini au point 3° se réfère à un événement qui cause ou est susceptible de causer une perturbation significative dans la fourniture d'un service essentiel. Les entités critiques doivent être capables de prévenir les incidents les touchant ou susceptibles de les toucher.

Le « service essentiel » défini au point 5° constitue « u*n service qui est crucial pour le maintien de fonctions sociétales ou d'activités économiques vitales, de la santé publique et de la sûreté publique, ou de l'environnement* ». Remarquons que, contrairement à la directive CER, le projet de loi rajoute, sous un point 6, la définition du « maintien de fonctions sociétales vitales ». Cette définition a été introduite afin de faire le lien entre le présent projet de loi et la loi modifiée du 23 juillet 2016 portant création d'un Haut-Commissariat à la Protection nationale.[6] En effet, cette loi relie la notion de la « crise » et de l'« entité critique » en les définissant à travers la sauvegarde des intérêts vitaux et des besoins essentiels de tout ou partie du pays ou de la population. Afin de garder cette cohérence entre les différents domaines d'attribution du Haut-Commissariat à la Protection nationale, le présent projet de loi rajoute les intérêts vitaux et les besoins essentiels du pays et de la population dans la définition des fonctions sociétales vitales.

Le point 9° reprend la définition de l'« entité de l'administration publique ». Faute de définition de l'administration publique dans le droit luxembourgeois, la référence au droit national a été omise dans le texte de transposition.

---

[4] Directive 2008/114/CE du Conseil du 8 décembre 2008 concernant le recensement et la désignation des infrastructures critiques européennes ainsi que l'évaluation de la nécessité d'améliorer leur protection, *J.O.U.E.*, L 345 du 23 décembre 2008.

[5] Consid. (2) et (3) directive CER.

[6] Loi modifiée du 23 juillet 2016 ponant création d'un Haut-Commissariat a la Protection nationale, *Mém. A* n° 137, 28 juillet 2016, p. 2342.

Ad article 3

L'article 3 détermine les autorités compétentes chargées de veiller à l'application correcte du présent projet de loi. D'une 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, ainsi que pour le secteur des infrastructures numériques pour les activités qui tombent sous la surveillance de la Commission de surveillance du secteur financier, telles que les activités des PSF de support. D'autre part, vu que le Haut-Commissariat à la Protection nationale (HCPN) est, depuis l'entrée en vigueur du règlement grand-ducal du 12 mars 2012[7] et de la loi du 23 juillet 2016[8], l'autorité compétente en matière d'infrastructures critiques nationales et européennes, la loi sous projet s'insère dans cette logique en lui attribuant la fonction d'autorité compétente pour les secteurs pour lesquels la CSSF n'a aucune compétence (énergie, transports, santé, eau potable, eaux résiduaires, activités des infrastructures numériques pour lesquelles la CSSF n'a aucune compétence, administration publique, espace, production, transformation et distribution de denrées alimentaires, gestion des déchets).

Afin d'assurer une bonne coopération entre les autorités compétentes et d'assurer une approche cohérente en matière de désignation des entités critiques et d'évaluation de leur résilience, l'alinéa 3 de l'article 3 prévoit une exception au secret professionnel inscrite dans la loi portant organisation de la CSSF, afin de permettre aux autorités compétentes de s'échanger des informations en cas de besoin.

Ad article 4

Le projet de loi accorde la mission de point de contact unique au 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 HCPN assure la coordination de la communication et la liaison avec les autorités compétentes nationales, ainsi qu'avec les points de contact uniques des autres États membres et le groupe sur la résilience des entités critiques, constitué au niveau de l'Union européenne.[9]

Ad article 5

L'article 5 prévoit que le HCPN élabore, après consultation de la CSSF, une stratégie visant à renforcer la résilience des entités critiques couvrant au moins les secteurs et sous-secteurs visés à l'annexe du projet de loi. La stratégie vise à garantir une approche globale de la résilience des entités critiques en définissant les objectifs stratégiques et les mesures politiques à mettre en œuvre. Dans un souci de cohérence et d'efficacité, la stratégie intégrera harmonieusement les politiques existantes, en s'appuyant sur des stratégies nationales et sectorielles, des plans ou des documents similaires pertinents existants[10], tels que :

- la stratégie nationale de cybersécurité 2021-2025 ;
- la stratégie pour l'adaptation aux effets du changement climatique au Luxembourg 2018-2023 ;
- la stratégie nationale à long terme en matière d'action climat « Vers la neutralité climatique en 2050 » ;
- la stratégie nationale en matière d'hydrogène, la stratégie nationale biogaz ;

[7] Règlement grand-ducal du 12 mars 2012 portant application de la directive 2008/114/CE du Conseil du 8 décembre 2008 concernant le recensement et la désignation des infrastructures critiques européennes ainsi que l'évaluation de la nécessité d'améliorer leur protection, *Mém. A* n° 45, 15 mars 2012, p. 449.

[8] Loi modifiée du 23 juillet 2016, *o.c.*, (v. note 6).

[9] Consid. (23) directive CER.

[10] Consid. (13) directive CER.

- la stratégie « Null Offall Lëtzebuerg » ;
- la stratégie pour une mobilité durable (2018-2025) ;
- la stratégie nationale pour les réseaux à ultra-haut débit 2021-2025 ;
- les Lignes directrices de la Défense luxembourgeoise à l'horizon 2035.

Un élément important de la stratégie est le cadre d'action pour une coordination renforcée entre les autorités compétentes en vertu du présent projet de loi et les autorités compétentes en vertu de la directive NIS 2. 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 et d'inciter une collaboration au niveau de l'exercice des tâches de supervision.[11]

Cette stratégie fera l'objet d'une révision et d'une mise à jour au moins tous les quatre ans.

Ad. article 6

L'article 6 prévoit que le HCPN effectue une évaluation des risques sur base des services essentiels identifiés par la Commission européenne. En effet, le HCPN est l'unique autorité compétente pour effectuer l'évaluation des risques et ce peu importe le secteur concerné. Cette approche va de pair avec la compétence du HCPN au niveau de la gestion de crise, qui s'étend sur tous secteurs confondus.

Cette évaluation des risques tient d'abord compte de l'analyse des risques générale que le HCPN effectue en vertu de sa loi-cadre[12] et qui prend en considération les risques naturels et d'origine humaine pertinents, y compris ceux qui revêtent un caractère transsectoriel ou transfrontière, les accidents d'envergure, les catastrophes naturelles, les urgences de santé publique, telles que les pandémies et les menaces hybrides et autres menaces antagonistes, telles que le risque terroriste, l'infiltration par les réseaux criminels et le sabotage.

Lorsqu'il procède à une telle évaluation, le HCPN tient aussi compte d'autres évaluations des risques générales ou sectorielles effectuées en vertu d'autres actes juridiques de l'Union et examine la mesure dans laquelle les secteurs dépendent les uns des autres, y compris de secteurs d'autres États membres et de pays tiers. Les résultats de l'évaluation des risques sont utilisés aux fins de recenser les entités critiques.[13]

Ad article 7

L'article 7 décrit le processus de recensement et de désignation des entités critiques pour les secteurs et sous-secteurs visés à l'annexe du projet de loi. Ce processus a pour objet de garantir que toutes les entités critiques soient soumises aux exigences en matière de résilience posées par la présente loi sous projet et de réduire les divergences à cet égard.[14]

A l'instar de la loi du 23 juillet 2016, les entités critiques sont désignées moyennant arrêté grand-ducal.[15]

Plusieurs critères cumulatifs entrent en compte dans le processus de recensement :

- D'abord, ne sont recensées que les entités qui fournissent un ou plusieurs services essentiels, c'est-à-dire « *un service qui est crucial pour le maintien de fonctions sociétales ou d'activités économiques vitales, de la santé publique et de la sûreté publique, ou de l'environnement* ».[16]
- Ensuite, il faut que l'entité exerce ses activités sur le territoire du Grand-Duché et que son infrastructure critique soit située sur ledit territoire. Une entité est considérée comme

[11] Consid. (13) directive CER.

[12] V. art. 3, para. 1er, point 3, de la loi modifiée du 23 juillet 2016, *o.c.*, (v. note 6).

[13] Consid. (15) directive CER.

[14] Consid. (16) directive CER.

[15] Art. 7 de la loi modifiée du 23 juillet 2016, *o.c.*, (v. note 6).

[16] Art. 2, point 5, du projet de loi.

exerçant des activités sur le territoire de l'État membre dans lequel elle exerce les activités nécessaires pour le ou les services essentiels en question et dans lequel se trouve l'infrastructure critique de cette entité, qui est utilisée pour fournir ce ou ces services.[17]

- Finalement, une entité est critique si un incident a des effets perturbateurs importants soit sur la fourniture d'un ou de plusieurs services essentiels, soit sur la fourniture d'autres services essentiels dans les secteurs figurant à l'annexe qui dépendent dudit ou desdits services essentiels.

L'alinéa 2 du paragraphe 2 exige la mise à disposition par les entités critiques de toutes les données nécessaires pour le recensement, la désignation et la protection desdites entités. Dans le but de maintenir une cohérence entre le régime actuel applicable aux infrastructures critiques et le futur régime applicable aux entités critiques, le paragraphe 2 est rédigé en s'inspirant de l'article 6, paragraphe 1er, de la loi portant création d'un Haut-Commissariat à la Protection nationale. L'article précité sera abrogé lorsque le présent projet entrera en vigueur.

Le paragraphe 3 fixe les critères à prendre en compte afin de déterminer l'importance de l'effet perturbateur causé par un incident en vue du recensement des entités critiques. Les critères en question répondent en grande partie aux critères inscrits dans le règlement grand-ducal du 21 février 2018 déterminant les modalités du recensement et de la désignation des infrastructures critiques. Ces critères sont appréciés et analysés en fonction des spécificités de chaque secteur par un des groupes de travail interministériels qui procèdent à l'identification des infrastructures critiques en vue de leur désignation par arrêté grand-ducal.

Notons que, vu que les infrastructures critiques recensées et désignées en application de la loi modifiée du 23 juillet 2016[18] répondent toutes aux critères ci-avant, celles-ci seront considérées comme entités critiques en vertu de la présente loi en projet.

Le paragraphe 4 exige, d'une part, que les autorités compétentes dressent une liste des entités recensées et désignées critiques et, d'autre part, que les entités critiques reçoivent une notification les informant de leur statut d'entité critique endéans un mois à compter de leur désignation. En outre, ces entités sont informées des obligations qui leur incombent en vertu des chapitres 4 et 5. Remarquons que les entités critiques des secteurs figurant aux points 3 et 4 de l'annexe, ainsi que les entités critiques figurant au point 8 de l'annexe pour les activités qui tombent sous la surveillance de la Commission de surveillance du secteur financier, ne sont pas soumises à ces obligations. Ce bout de phrase est en étroite relation avec le libellé de l'article 8 et sera donc approfondi dans le commentaire de cet article.

Le paragraphe 5 vise le cas spécial de l'entité critique qui fournirait des services essentiels à ou dans six États membres ou plus. En effet, puisque les entités critiques exercent leurs activités dans le cadre d'un réseau de fourniture de services et d'infrastructures de plus en plus interconnecté et fournissent souvent des services essentiels dans plus d'un État membre, certaines de ces entités critiques revêtent une importance particulière pour l'Union et son marché intérieur. Ainsi, afin de tenir compte de cette réalité, la directive et le projet de loi ont introduit la notion d'« entité critique d'importance européenne particulière » et accordent à celle-ci un soutien renforcé au niveau de l'Union, telles que les missions de conseil[19]. Au niveau du recensement, si une entité critique se retrouve à fournir des services essentiels dans six États membres différents au moins, ladite entité en informe, conformément au paragraphe 5, son autorité compétente.

Afin d'assurer la cohérence entre la transposition de la directive CER et la directive NIS 2, les autorités compétentes notifient aux autorités compétentes de la directive NIS 2 l'identité des entités critiques qu'ils ont recensées et désignées.

Finalement, le paragraphe 7 prévoit une revue régulière de la liste des entités critiques.

---

[17] Consid. (16) directive CER.

[18] Loi modifiée du 23 juillet 2016, *o.c.*, (v. note 6).

[19] Consid. (35) directive CER.

Ad article 8

L'article 8 a été reformulé conformément à la recommandation du Conseil d'État dans son deuxième avis complémentaire du 8 décembre 2025 concernant la désignation des entités de l'administration publique exerçant leurs activités dans le domaine de la sécurité nationale et de la défense qui sont exclues du champ d'application de ce projet de loi. La formulation est inspirée de la voie choisie par le législateur belge et désigne nommément les entités 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.[20]

Pour rappel, 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 en 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.

En ce qui concerne les infrastructures numériques visées par le point 8 du tableau en annexe, les auteurs du projet de loi estiment que la directive devrait leur être partiellement applicable lorsque leur activité tombe sous la surveillance de la CSSF. Ces activités sont, en effet, entièrement couvertes par les dispositions du secteur financier, énoncées ci-dessus. En ce qui concerne les activités des infrastructures numériques qui ne tombent pas sous la surveillance de la CSSF, la présente loi sous projet leur devrait être pleinement applicable, dans la mesure où la directive CER donne la possibilité aux États membres d'adopter ou de maintenir des dispositions de droit national afin d'atteindre un niveau de résilience plus élevé. Alors qu'il est vrai que ces activités tombent sous l'égide de la loi portant transposition de la directive NIS 2, celle-ci ne visera que la résilience cybernétique.

Si dans le futur, il y avait des législations sectorielles qui s'appliquaient aux infrastructures numériques, dont l'activité ne tombe pas sous la surveillance de la CSSF, et qui avaient un effet au moins équivalent aux obligations du projet de loi sous rubrique, l'article 1er, paragraphe 2, aurait pour effet de dispenser l'application du projet de loi à ces entités.

Ad article 9

Sans préjudice de la propre responsabilité juridique qui incombe aux entités critiques de garantir le respect des obligations prévues par le projet de loi, les autorités compétentes aident les entités critiques à renforcer leur résilience. En particulier, lesdites autorités élaborent des documents d'orientation et des méthodologies, apportent leur soutien à l'organisation d'exercices visant à tester la résilience des entités critiques, dispensent des formations et fournissent des conseils au personnel des entités critiques.[21]

Il est à noter que déjà à l'heure actuelle, le HCPN apporte un soutien aux infrastructures critiques. En effet, sont actuellement en place :

[20] *M.B.*, 17 mai 2024, p. 63179.
[21] Consid. (25) directive CER.

- un guide pour l'élaboration d'un plan de sécurité et de continuité de l'activité ;
- des recommandations sectorielles sur la protection, la continuité de l'activité, la gestion de crise et la résilience ;
- des recommandations sur les mesures de protection, de continuité de l'activité, de gestion de crise et de résilience contenues dans les plans de sécurité et de continuité de l'activité de différents opérateurs d'infrastructures critiques ; des guides pour la protection et la résilience face à des risques spécifiques (intempéries, inondation, …) ;
- des colloques d'échanges sur les retours d'expériences et les leçons apprises entre opérateurs d'infrastructures critiques ;
- des conseils particuliers sur demandes ponctuelles des opérateurs ; et
- le partage de lettres de veille, telles que la newsletter « Critical Infrastructure Resilience : News, Updates and Events » de la Commission européenne, avec les opérateurs d'infrastructures critiques.

Ad article 10

L'article 10 règle la coopération entre États membres dans les cas où une entité critique exerce ses activités dans plusieurs États membres. Dans cette hypothèse, il importe de transmettre des exigences convergentes aux entités critiques afin que celles-ci puissent augmenter leur résilience sans pour autant accroître leur charge administrative.[22]

Ad article 11

L'article 11 impose aux entités critiques de procéder à une évaluation des risques. En effet, afin de pouvoir augmenter leur résilience, ces entités doivent avoir une connaissance approfondie des risques pertinents auxquels elles sont exposées. À cette fin, elles procèdent à une première évaluation des risques neuf mois suivant la réception de la notification qui les informe qu'elles ont été désignées en tant qu'entité critique. Ensuite, cette évaluation des risques est mise à jour chaque fois que cela s'avère nécessaire compte tenu de leurs circonstances particulières et de l'évolution de ces risques et, en tout cas, tous les quatre ans.[23]

Ad article 12

Après avoir évalué les risques les concernant, l'article 12 du projet de loi invite les entités critiques à mettre en place des mesures techniques, des mesures de sécurité et des mesures organisationnelles appropriées et proportionnées aux risques auxquels elles sont confrontées. Les mesures en question répondent en grande partie aux mesures que les infrastructures critiques doivent déjà aujourd'hui détailler et mettre en place en vertu des plans de continuité et de sécurité de l'activité prévus à l'article 8 de la loi modifiée du 23 juillet 2016 portant création d'un Haut-Commissariat à la Protection nationale.

D'abord, ces mesures sont destinées à prévenir tout incident et à s'en protéger. En ce qui concerne la protection physique de l'infrastructure, les entités peuvent prendre en considération, par exemple, des clôtures, des barrières, des outils et procédures de surveillance des enceintes, et des équipements de détection et de contrôle des accès.[24] Ensuite, les mesures techniques visent à réagir et à résister aux incidents et devront servir à faire une gestion adéquate de la sécurité liée au personnel. Finalement, il faut que ces mesures permettent à l'entité de se remettre des incidents. Il découle en outre de l'article que le personnel de l'entité devra être sensibilisé adéquatement des mesures mises en place.

Le paragraphe 2 dispose que les entités critiques devront décrire les mesures qu'elles prennent avec un niveau de détail suffisant, eu égard aux risques identifiés, dans un plan de

[22] Consid. (26) directive CER.

[23] Consid. (28) directive CER.

[24] Art. 13, para. 1er, lettre b), directive CER.

résilience ou dans un ou plusieurs documents équivalents, et appliquer ce plan dans la pratique. A l'instar de ce qui est prévu pour l'évaluation des risques effectuée par les entités critiques et pour éviter les doubles emplois, l'article 12 permet aux entités critiques d'utiliser les mesures prises en vertu d'autres actes juridiques, afin de satisfaire aux exigences du présent article. Notons que la directive énonce quelques exemples de mesures dans les domaines de l'aviation, du transport maritime, du réseau routier et du secteur ferroviaire qui pourraient satisfaire à ces exigences.[25]

Ad article 13

L'article 13 met en place un système de vérification des antécédents pour des catégories spécifiques de personnel employé par les entités critiques, visées dans au paragraphe 1er, afin de pallier le risque que des membres du personnel utilisent, par exemple, de manière abusive leurs fonctions ou encore leurs droits d'accès au sein de l'organisation de l'entité critique.

Plus précisément, à l'instar du système de vérification des antécédents mis en place par la loi modifiée du 18 juillet 2018 sur la Police grand-ducale,[26] le règlement grand-ducal du 28 juillet 2018 portant exécution de l'article 26 de la loi du 18 juillet 2018 sur la Police grand-ducale pour les institutions de l'Union européenne[27] et le projet de loi n° 7475[28] et son projet de règlement grand-ducal d'exécution,[29] la Police grand-ducale est l'autorité étatique en charge des demandes de vérification des antécédents introduites par les entités critiques. Ainsi, la Police grand-ducale est à considérer comme responsable du traitement au sens de la législation sur la protection des données à caractère personnel. Avec la compétence de la Police grand-ducale, ce système se distingue fondamentalement des procédures de « contrôle d'honorabilité » mises en place par le projet de loi n° 7691[30] qui confient cette mission au Ministre de la Justice, voire au procureur général d'État.

Le paragraphe 1er reprend la finalité du traitement, à savoir l'évaluation du risque potentiel pour la sécurité de l'entité concernée, et les catégories de personnes occupant une fonction sensible au sein de l'entité pour lesquelles une demande de vérification des antécédents peut être introduite. En vertu de l'article 12, paragraphe 1er, point 5, l'entité critique devra informer l'autorité compétente quelles fonctions considérées « sensibles » au sein de son entité nécessitent une vérification des antécédents. Vu qu'il reviendra à l'autorité compétente, dans sa fonction de supervision, de se prononcer par rapport aux mesures de résilience proposées par l'entité critique en vertu de l'article 12, le texte sous projet précise que les catégories de personnes au sujet desquelles une vérification est demandée devront, préalablement à l'introduction de la demande, faire l'objet d'un avis favorable par l'autorité compétente. Les auteurs du projet de loi veulent ainsi s'assurer, à travers les entités critiques, d'une certaine

[25] Consid. (31) directive CER.

[26] Art. 26 de la loi modifiée du 18 juillet 2018 sur la Police grand-ducale, *Mém. A* n° 621, 28 juillet 2018.

[27] Règlement grand-ducal du 28 juillet 2018 portant exécution de l'article 26 de la loi du 18 juillet 2018 sur la Police grand-ducale pour les institutions de l'Union européenne, *Mém. A* n° 647, 3 août 2018.

[28] Projet de loi portant modification de la loi modifiée du 26 juillet 2002 sur la police et sur l'exploitation de l'aéroport de Luxembourg ainsi que sur la construction d'une nouvelle aérogare, *doc. parl.* n° 7475.

[29] Projet de règlement grand-ducal relatif à la sûreté de l'aviation civile et aux conditions d'accès à l'aéroport de Luxembourg.

[30] Projet de loi portant modification 1° du Code de procédure pénale 2° du Nouveau Code de procédure civile 3° de la loi du 7 juillet 1971 portant en matière répressive et administrative, institution d'experts, de traducteurs et d'interprètes assermentés et complétant les dispositions légales relatives à l'assermentation des experts, traducteurs et interprètes 4° de la loi modifiée du 9 décembre 1976 relative à l'organisation du notariat 5° de la loi modifiée du 20 avril 1977 sur les jeux de hasard et les paris sportifs 6° de la loi modifiée du 7 mars 1980 sur l'organisation judiciaire 7° de la loi modifiée du 7 novembre 1996 portant organisation des juridictions de l'ordre administratif 8° de la loi du 30 décembre 1981 portant indemnisation en cas de détention préventive inopérante 9° de la loi modifiée du 15 mars 1983 sur les armes et munitions 10° de la loi modifiée du 2 mars l984 relative à l'indemnisation de certaines victimes de dommages corporels résultant d'une infraction et à la répression de l'insolvabilité frauduleuse 11° de la loi modifiée du 4 décembre 1990 portant organisation du service des huissiers de justice 12° de la loi du 31 janvier 1998 portant agrément des services d'adoption et définition des obligations leur incombant 13° de la loi du 6 mai 1999 relative à la médiation pénale et portant modification de différentes dispositions a) de la loi modifiée du 7 mars 1980 sur l'organisation judiciaire, b) du code des assurances sociales 14° de la loi du 12 novembre 2002 relative aux activités privées de gardiennage et de surveillance 15° de la loi modifiée du 7 juin 2012 sur les attachés de justice, *doc. parl.* n° 7691[7].

cohérence par rapport aux catégories de personnes au sujet desquelles une vérification des antécédents est demandée.

Le paragraphe 2 se base sur le système mis en place par le projet de loi n° 7475 en énumérant les informations qui devront figurer dans le dossier introduit par l'entité critique. Notons que cette énumération a été largement reprise du projet de règlement grand-ducal portant exécution du projet de loi n° 7475.

D'après le paragraphe 3, la Police grand-ducale procède à la vérification des antécédents sur une période de cinq ans précédant la demande.

Finalement, le paragraphe 4 reproduit les critères d'échec à la vérification des antécédents afin de couvrir tous les risques que la personne visée au paragraphe 1er pourrait représenter pour la sécurité de l'entité critique. Cet avis de la Police grand-ducale sera transmis au ministre ayant la Protection nationale dans ses attributions.

Ad article 14

Le paragraphe 1er vise à faire face à l'absence de procédure au terme de la vérification des antécédents effectuée par la Police grand-ducale. En effet, en prenant en considération l'avis de la Police grand-ducale, il appartiendra au ministre ayant la Protection nationale dans ses attributions d'émettre une décision relative au risque potentiel que la personne visée à l'article 13, paragraphe 1er, représente pour la sécurité de l'entité critique.

Le ministre ayant la Protection nationale dans ses attributions notifiera ensuite sa décision motivée à la personne faisant l'objet de la vérification des antécédents (paragraphe 2).

Ledit ministre transmettra également sa décision à l'entité requérante, sans lui communiquer les données personnelles qu'il a reçues dans l'avis de la Police grand-ducale. L'entité critique requérante est tenue de suivre la décision du ministre (paragraphe 3).

Le paragraphe 4, inspiré de l'article 17, paragraphe 8, de la loi du 7 août 2023 sur l'organisation de l'Armée luxembourgeoise, porte sur le recours dont disposera la personne concernée contre les décisions qui sont prises à son encontre et de l'accès au dossier qui a été constitué dans le cadre de la vérification des antécédents.

Ad article 15

L'article 15 autorise la mise en place d'un système informatique centralisé permettant la gestion administrative des demandes de vérification des antécédents et règle la protection des données personnelles des personnes soumises à une vérification des antécédents. Le projet de loi essaye de trouver un équilibre entre le droit de la personne soumise à la vérification et la nécessité pour la Police grand-ducale d'avoir accès aux vérifications antérieurement effectuées. Ainsi, la loi prévoit que la Police conserve les données concernées pendant une année à partir de la notification de l'avis à l'entité critique.

Ad article 16

L'article 16 met en place un mécanisme de notification d'incidents afin de permettre aux autorités compétentes de réagir rapidement et de manière adéquate aux incidents d'une certaine importance et de disposer d'une vue d'ensemble complète de l'impact, de la nature, de la cause et des conséquences éventuelles d'incidents auxquels les entités critiques sont confrontées.[31]

Ainsi, les entités critiques notifient, sans retard injustifié, aux autorités compétentes les incidents qui perturbent ou sont susceptibles de perturber de manière importante la fourniture de services essentiels. Alors que le texte du projet de loi précise trois critères à prendre en

[31] Consid. (33) directive CER.

compte pour déterminer l'importance de la perturbation, il est prévu qu'un règlement grand-ducal précisera ces critères pour chaque secteur retenu en annexe.

À moins qu'elles n'en soient empêchées sur le plan opérationnel, les entités critiques présentent une notification initiale au plus tard vingt-quatre heures après avoir pris connaissance d'un incident. La notification initiale ne devrait inclure que les informations strictement nécessaires pour porter l'incident à la connaissance de l'autorité compétente et permettre à l'entité critique de demander une assistance, si nécessaire. Une telle notification devrait indiquer, lorsque cela est possible, la cause présumée de l'incident. La notification initiale est suivie, s'il y a lieu, d'un rapport détaillé au plus tard un mois après l'incident. Le rapport détaillé devrait compléter la notification initiale et fournir une vue d'ensemble plus complète de l'incident.[32]

Ad article 17

Alors que le projet de loi ne reprend pas le détail des obligations qui incombent à la Commission européenne dans ce contexte, l'article 17 se limite, dans son paragraphe 1er, à définir les entités critiques d'importance européenne particulière et impose à celles-ci d'accorder aux missions de conseil organisées par la Commission accès à leurs informations, systèmes et installations, en son paragraphe 2.

Ad article 18

Afin que la bonne application et l'exécution de la présente loi sous projet soient assurées, le paragraphe 1er dispose que les autorités compétentes jouissent du pouvoir d'effectuer des inspections et des audits, de superviser les mesures mises en place par les entités critiques, voire d'exiger des entités critiques qu'elles fournissent des informations et des éléments de preuve concernant les mesures qu'elles ont prises pour respecter leurs obligations et, lorsque c'est nécessaire, d'adresser des injonctions afin qu'il soit remédié aux violations constatées.

L'alinéa 2 du paragraphe 1er encadre les pouvoirs de police administrative prévus par le premier alinéa. Ainsi, les inspections ne peuvent avoir lieu qu'à des plages horaires prédéfinies, moyennant préavis de deux semaines, par un agent des groupes de traitement ou d'indemnité A1 ou A2 de l'autorité compétente. Ces inspections pourront aussi se dérouler en dehors des plages horaires prédéfinies dans le présent projet avec l'accord de l'entité critique. Notons que, puisque le chapitre 6 sur la supervision et l'exécution ne s'applique au secteur bancaire, aux infrastructures des marchés financiers et aux infrastructures numériques pour lesquels la CSSF est l'autorité compétente, seul le HCPN sera concerné par ces inspections.

Dans un souci de transparence, il est prévu que lorsqu'ils procèdent à une inspection, les agents du HCPN signalent leur présence à l'agent de liaison désigné par l'entité critique en vertu de l'article 12, paragraphe 3, du projet de loi. L'agent de liaison peut accompagner les agents du HCPN lors de l'inspection. Cet article s'inspire de la loi modifiée du 19 mai 1999[33] qui prévoit des garanties similaires dans le cadre de pouvoirs de contrôle accordés aux agents de la Direction de l'aviation civile.

Finalement, les agents procédant à l'inspection dressent un rapport relatif à l'inspection opérée, qui est transmis à l'agent de liaison de l'entité.

Le paragraphe 2 fait le lien entre la directive CER et la directive NIS 2. En effet, comme évoqué précédemment, il se pourrait qu'une entité essentielle sous l'égide de la directive NIS 2 soit aussi recensée en tant qu'entité critique. Ainsi, ces entités sont tenues de fournir aux

[32] Consid. (33) directive CER.

[33] Art. 19*bis*, para. 4, de la loi 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, *Mém. A* n°57, 21 mai 1999, p. 1339.

autorités compétentes les informations nécessaires pour évaluer leurs mesures de résilience, ainsi que des éléments prouvant la mise en œuvre effective de ces mesures.

Dans un but de cohérence entre le régime actuellement applicable aux infrastructures critiques et le futur régime applicable aux entités critiques, la formulation du paragraphe 2, alinéa 1er, s'inspire du libellé de l'article 6 de la loi portant création d'un Haut-Commissariat à la Protection nationale qui sera abrogé avec l'entrée en vigueur du présent projet.[34] Dans la même lignée, le deuxième alinéa du paragraphe 2 est repris de la même loi du 23 juillet 2016. Cette disposition permettra au HCPN, qui porte la double casquette de gestionnaire de crises et d'autorité compétente en matière d'entités critiques, de faire le lien entre ces deux compétences.

Le paragraphe 3 permet aux autorités compétentes d'adresser des injonctions aux entités critiques afin que celles-ci remédient aux violations constatées au présent projet de loi. A nouveau, cette disposition trace un parallélisme avec l'article 9, paragraphe 2, de la loi du 28 mai 2019,[35] qui impose un régime similaire aux opérateurs de services essentiels. Ainsi, le projet de loi vise à instaurer une égalité de traitement entre entités critiques et opérateurs de services essentiels.

Les pouvoirs dont les autorités compétentes jouissent en vertu des paragraphes 1er à 3 ne peuvent s'exercer que sous réserve de garanties appropriées. Ainsi, ces pouvoirs devront être exercés de manière objective, transparente et proportionnée, tout en tenant compte des droits et des intérêts légitimes des entités critiques concernées, tels que la protection des secrets commerciaux et d'affaires, le droit d'être entendu, les droits de la défense et le droit à un recours effectif devant une juridiction indépendante.[36]

Le paragraphe 4 prévoit que lorsqu'elles évaluent le respect par les entités critiques des obligations que leur impose la présente loi sous projet, les autorités compétentes peuvent demander aux autorités compétentes en vertu de la directive NIS 2 d'exercer leurs pouvoirs de supervision et d'exécution à l'égard d'une entité relevant de ladite directive qui a été désignée en tant qu'entité critique en vertu du présent projet de loi.

Ad article 19

Afin d'assurer que la présente loi soit appliquée en pratique, il y a lieu de l'assortir de sanctions administratives adéquates. Ainsi, l'autorité compétente peut décider des sanctions à l'encontre des entités critiques si elles ne se conforment pas aux prescriptions des articles 11, 12, 14,16, 17 et 18.

Remarquons que les sanctions administratives énumérées dans l'article 19 et la procédure y relative s'inspirent fortement de la législation existante dans le secteur des opérateurs des services essentiels.[37]

Ad article 20

L'article 20 procède à des modifications de la loi-cadre du Haut-Commissariat à la Protection nationale afin d'y intégrer le nouveau vocabulaire, d'une part, et de procéder à des adaptations ponctuelles devenues nécessaires, d'autre part.

En ce qui concerne les entités critiques, l'article 20 remplace d'abord la notion d'« infrastructure critique » par celle d'« entité critique » à travers le texte de la loi du Haut-Commissariat à la Protection nationale, afin d'accorder une suite au nouveau vocabulaire introduit par la directive CER. Dans la même optique, le point 3° reformule et adapte les missions du HCPN en matière d'entités critiques à la terminologie instaurée par la directive. Enfin, le projet de loi abroge les articles 4 à 8 relatifs aux infrastructures critiques. En effet,

[34] Loi modifiée du 23 juillet 2016, *o.c.*, (v. note 6), art. 6, al. 1er.

[35] Loi du 28 mai 2019 portant transposition de la directive (UE) 2016/1148, *o.c.*, (v. note 3).

[36] Art. 21, para. 4, directive CER.

[37] Art. 14 de la loi du 28 mai 2019 portant transposition de la directive (UE) 2016/1148, *o.c.*, (v. note 3).

alors que la législation sur les infrastructures critiques faisait, depuis 2016, partie intégrante de la loi organique du Haut-Commissariat à la Protection nationale, il a été jugé plus logique de transposer la directive CER avec une loi spéciale à part entière, d'autant plus que le HCPN se partagera dorénavant le rôle de l'autorité compétente avec la Commission de surveillance du secteur financier. L'article 9, dernière disposition du chapitre relatif aux infrastructures critiques, restera dans la loi organique du HCPN, puisqu'il règle la situation des entités critiques en cas de crise.

Ad article 21

L'article 21 introduit un intitulé de citation, afin de faciliter la référence à la présente loi sous projet.

Annexe

L'annexe du projet de loi a été repris de l'annexe de la directive CER. L'unique différence consiste dans le fait qu'au-delà des secteurs prévus par la directive, l'annexe du projet ajoute la « gestion des déchets » comme douzième secteur. Comme ce secteur est déjà à l'heure actuelle un secteur dans lequel sont recensées des infrastructures critiques[38] et comme ce secteur joue et continuera à jouer un rôle essentiel, il a été décidé de l'ajouter à la liste des secteurs.

VI. Texte proposé par la Commission

Sous le bénéfice des observations qui précèdent, la Commission recommande à la Chambre des Députés d'adopter le projet de loi n° 8307 dans la teneur qui suit :

PROJET DE LOI

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

Chapitre 1er – Champ d'application et définitions

Art. 1er. (1) La présente loi ne s'applique pas aux questions couvertes par la loi du XXX concernant des mesures destinées à assurer un niveau élevé de cybersécurité, sans préjudice de l'article 8.

(2) Lorsque des dispositions d'actes juridiques sectoriels de l'Union européenne exigent des entités critiques qu'elles adoptent des mesures pour renforcer leur résilience, et lorsque ces exigences ont un effet au moins équivalent aux obligations correspondantes prévues par la présente loi, les dispositions pertinentes de la présente loi, y compris les dispositions relatives à la supervision et à l'exécution prévues au chapitre 6, ne s'appliquent pas.

La liste des actes juridiques sectoriels de l'Union européenne ayant un effet au moins équivalent à la présente loi est arrêtée par règlement grand-ducal.

[38] Art. 1er, point 6, du règlement grand-ducal du 21 février 2018 déterminant les modalités du recensement et de la désignation des infrastructures critiques, *Mém. A* n°152, 1er mars 2018.

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

1° « entité critique » : une entité publique ou privée qui a été désignée conformément à l'article 7 comme appartenant à l'une des catégories qui figurent dans la troisième colonne du tableau de l'annexe ;

2° « résilience » : la capacité d'une entité critique à prévenir tout incident, à s'en protéger, à y réagir, à y résister, à l'atténuer, à l'absorber, à s'y adapter et à s'en rétablir ;

3° « incident » : un événement qui perturbe ou est susceptible de perturber de manière importante la fourniture d'un service essentiel, y compris lorsqu'il affecte les systèmes nationaux qui préservent l'état de droit ;

4° « infrastructure critique » : un bien, une installation, un équipement, un réseau ou un système, ou une partie d'un bien, d'une installation, d'un équipement, d'un réseau ou d'un système, qui est nécessaire à la fourniture d'un service essentiel ;

5° « service essentiel » : un service qui est crucial pour le maintien de fonctions sociétales ou d'activités économiques vitales, de la santé publique et de la sûreté publique, ou de l'environnement ;

6° « maintien de fonctions sociétales vitales » : la disponibilité de services indispensables à la sauvegarde des intérêts vitaux ou des besoins essentiels de tout ou partie du pays ou de la population ;

7° « 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 la probabilité que l'incident se produise ;

8° « évaluation des risques » : l'ensemble du processus permettant de déterminer la nature et l'étendue d'un risque en déterminant et en analysant les menaces, les vulnérabilités et les dangers potentiels pertinents qui pourraient conduire à un incident et en évaluant la perte ou la perturbation potentielle de la fourniture d'un service essentiel causée par cet incident ;

9° « 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 les autorités de l'État ou d'autres organismes de droit public de niveau central, ou 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, pour plus de la moitié, de membres désignés par les autorités de l'État ou d'autres organismes de droit public de niveau central ;

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.

Chapitre 2 – Autorités compétentes et point de contact national unique

Art. 3. La Commission de surveillance du secteur financier est l'autorité compétente chargée de veiller à l'application correcte de la présente loi pour le secteur bancaire et le secteur des infrastructures des marchés financiers, figurant aux points 3° et 4° du tableau de l'annexe, ainsi que le secteur des infrastructures numériques, figurant au point 8° du tableau de l'annexe, pour les activités qui tombent sous la surveillance de la Commission de surveillance du secteur financier.

Le Haut-Commissariat à la Protection nationale est l'autorité compétente chargée de veiller à l'application correcte de la présente loi pour les autres secteurs visés à l'annexe, ainsi que le secteur des infrastructures numériques, figurant au point 8° du tableau de l'annexe, pour les activités qui ne tombent pas 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 ne fait pas obstacle à l'échange d'informations confidentielles entre les autorités compétentes dans le cadre et aux seules fins de la présente loi et des mesures prises pour son exécution.

Art. 4. Le Haut-Commissariat à la Protection nationale constitue le point de contact national unique chargé d'exercer une fonction de liaison afin d'assurer la coopération transfrontière avec les points de contact uniques des autres États membres de l'Union européenne et avec le groupe sur la résilience des entités critiques visé à l'article 19 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. En outre, le point de contact national unique exerce une fonction de liaison avec la Commission européenne et assure la coopération avec les pays tiers.

Chapitre 3 – Cadre national pour la résilience des entités critiques

Art. 5. Le Haut-Commissariat à la Protection nationale élabore, après consultation de la Commission de surveillance du secteur financier, une stratégie visant à renforcer la résilience des entités critiques qui définit des objectifs stratégiques et des mesures politiques, en s'appuyant sur des stratégies nationales et sectorielles, des plans ou des documents similaires pertinents existants, en vue d'atteindre et de maintenir un niveau élevé de résilience des entités critiques et de couvrir au moins les secteurs figurant à l'annexe.

La stratégie contient les éléments suivants :

1° les objectifs stratégiques et les priorités aux fins de renforcer la résilience globale des entités critiques, compte tenu des dépendances et des interdépendances transfrontières et transsectorielles ;

2° un cadre de gouvernance permettant d'atteindre les objectifs stratégiques et les priorités, y compris une description des rôles et des responsabilités des différentes autorités, entités critiques et autres parties participant à la mise en œuvre de la stratégie ;

3° une description des mesures nécessaires pour renforcer la résilience globale des entités critiques, y compris une description de l'évaluation des risques visée à l'article 6 ;

4° une description du processus par lequel les entités critiques sont recensées ;

5° une description du processus de soutien aux entités critiques conformément au présent chapitre, y compris les mesures visant à renforcer la coopération entre le secteur public, d'une part, et le secteur privé et les entités publiques et privées, d'autre part ;

6° une liste des principales autorités et parties prenantes concernées, autres que les entités critiques, participant à la mise en œuvre de la stratégie ;

7° un cadre d'action pour la coordination entre les autorités compétentes au sens de la présente loi et les autorités compétentes en vertu de la loi du XXX concernant des mesures destinées à assurer un niveau élevé de cybersécurité aux fins du partage d'informations sur les risques, menaces et incidents en matière de cybersécurité ainsi que sur les risques, menaces et incidents non liés à la cybersécurité, et de l'exercice des tâches de supervision ;

8° une description des mesures déjà en place visant à faciliter la mise en œuvre des obligations prévues au chapitre 4 par les petites et moyennes entreprises au sens de l'annexe de la recommandation 2003/361/CE de la Commission du 6 mai 2003 concernant la définition des micro, petites et moyennes entreprises recensées en tant qu'entités critiques.

À la suite d'une consultation qui est, dans la mesure du possible en pratique, ouverte aux parties prenantes concernées, le Haut-Commissariat à la Protection nationale met à jour la stratégie au moins tous les quatre ans.

Art. 6. (1) Le Haut-Commissariat à la Protection nationale effectue une évaluation des risques sur base des services essentiels identifiés par la Commission européenne. Cette évaluation des risques est utilisée pour recenser les entités critiques conformément à l'article 7 et pour aider les entités critiques à adopter des mesures en vertu de l'article 12.

(2) Afin de procéder à l'évaluation des risques, le Haut-Commissariat à la Protection nationale tient compte des éléments suivants :

1° l'analyse des risques qui tient compte des risques naturels et d'origine humaine pertinents, y compris ceux qui revêtent un caractère transsectoriel ou transfrontière, des accidents, des catastrophes naturelles, des urgences de santé publique et des menaces hybrides ou autres menaces antagonistes, lesquelles comprennent les infractions terroristes prévues par le Code pénal ;

2° l'évaluation des risques générale effectuée en vertu de l'article 6, paragraphe 1er, de la décision n° 1313/2013/UE du Parlement européen et du Conseil du 17 décembre 2013 relative au mécanisme de protection civile de l'Union européenne ;

3° d'autres évaluations des risques pertinentes effectuées conformément aux exigences des actes juridiques sectoriels pertinents de l'Union européenne, y compris le règlement (UE) 2017/1938 du Parlement européen et du Conseil du 25 octobre 2017 concernant des mesures visant à garantir la sécurité de l'approvisionnement en gaz naturel et abrogeant le règlement (UE) n° 994/2010, tel que modifié, et le règlement (UE) 2019/941 du Parlement européen et du Conseil du 5 juin 2019 sur la préparation aux risques dans le secteur de l'électricité et abrogeant la directive 2005/89/CE, ainsi que la loi modifiée du 19 décembre 2008 relative à l'eau et la loi du 28 avril 2017 concernant la maîtrise des dangers liés aux accidents majeurs impliquant des substances dangereuses ;

4° les risques pertinents découlant de la mesure dans laquelle les secteurs figurant à l'annexe dépendent les uns des autres, y compris de la mesure dans laquelle ils dépendent d'entités situées dans d'autres États membres de l'Union européenne et des pays tiers, et l'incidence qu'une perturbation importante dans un secteur peut avoir sur d'autres secteurs, y compris tout risque important pour les citoyens et le marché intérieur ;

5° toute information sur les incidents notifiés conformément à l'article 16.

Aux fins de l'alinéa 1er, point 4°, le Haut-Commissariat à la Protection nationale coopère avec les autorités compétentes d'autres États membres de l'Union européenne en vertu 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 les autorités compétentes de pays tiers, s'il y a lieu.

(3) Le Haut-Commissariat à la Protection nationale met à la disposition des entités critiques recensées conformément à l'article 7, les éléments pertinents des évaluations des risques.

Art. 7. (1) Les autorités compétentes recensent les entités critiques et leurs infrastructures critiques afférentes pour les secteurs et sous-secteurs figurant à l'annexe, dans leurs champs de compétences respectifs.

La désignation d'une entité critique et de ses infrastructures critiques fait l'objet d'un arrêté grand-ducal.

(2) Lorsqu'une autorité compétente recense les entités critiques en vertu du paragraphe 1er, elle tient compte des résultats de l'évaluation des risques effectuée en vertu de l'article 6 et de la stratégie visée à l'article 5 et applique tous les critères suivants :

1° l'entité fournit un ou plusieurs services essentiels ;

2° l'entité exerce ses activités sur le territoire luxembourgeois et son infrastructure critique est située sur ledit territoire ; et

3° un incident aurait des effets perturbateurs importants, déterminés conformément au paragraphe 3, sur la fourniture par l'entité d'un ou de plusieurs services essentiels ou sur la fourniture d'autres services essentiels dans les secteurs figurant à l'annexe qui dépendent dudit ou desdits services essentiels.

L'entité critique est tenue de mettre à la disposition de l'autorité compétente toutes les données sollicitées aux fins du recensement, de la désignation et de la protection des entités critiques.

(3) L'importance d'un effet perturbateur visé au paragraphe 2, point 3°, est déterminée sur base des critères suivants :

1° le nombre d'utilisateurs tributaires du service essentiel fourni par l'entité concernée ;

2° la mesure dans laquelle les autres secteurs et sous-secteurs figurant à l'annexe dépendent du service essentiel en question ;

3° l'impact que des incidents pourraient avoir, du point de vue de l'ampleur et de la durée, sur les activités économiques et sociétales, l'environnement, la sûreté et la sécurité publiques, ou la santé de la population ;

4° la part de marché de l'entité sur le marché du ou des services essentiels concernés ;

5° la zone géographique susceptible d'être affectée par un incident, y compris toute incidence transfrontière, compte tenu de la vulnérabilité associée au degré d'isolement de certains types de zones géographiques ;

6° l'importance que revêt l'entité pour le maintien d'un niveau suffisant de service essentiel, compte tenu de la disponibilité de solutions de rechange pour la fourniture de ce service essentiel.

(4) Les autorités compétentes dressent une liste des entités critiques recensées et désignées en vertu du paragraphe 2 et informent ces entités critiques qu'elles ont été désignées en tant qu'entité critique dans un délai d'un mois à compter de cette désignation. Les autorités compétentes informent ces entités critiques des obligations qui leur incombent en vertu des chapitres 4 et 5 et de la date à partir de laquelle ces obligations leur sont applicables, sans préjudice de l'article 8. Les autorités compétentes informent les entités critiques des secteurs figurant aux points 3° et 4° du tableau de l'annexe qu'elles ne sont soumises à aucune des obligations prévues aux chapitres 4 et 5. De même, les autorités compétentes informent les entités critiques du secteur figurant au point 8° du tableau de l'annexe qu'elles ne sont soumises à aucune des obligations prévues aux chapitres 4 et 5, pour les activités qui tombent sous la surveillance de la Commission de surveillance du secteur financier.

Le chapitre 4 s'applique aux entités critiques concernées à l'expiration d'un délai de dix mois à compter de la date de la notification visée à l'alinéa 1er.

(5) L'entité critique, à la suite de la notification visée au paragraphe 4, informe son autorité compétente lorsqu'elle fournit des services essentiels à ou dans six États membres de l'Union européenne ou plus. En pareil cas, l'entité critique informe son autorité compétente au sujet des services essentiels qu'elle fournit à ou dans ces États membres et au sujet des États membres auxquels ou dans lesquels elle fournit ces services essentiels. Les dispositions du chapitre 5 s'appliquent.

(6) Les autorités compétentes notifient aux autorités compétentes en vertu de la loi du XXX concernant des mesures destinées à assurer un niveau élevé de cybersécurité l'identité des entités critiques qu'ils ont recensées et désignées dans un délai d'un mois à compter de la désignation. Cette notification précise, le cas échéant, que les entités critiques concernées sont des entités des secteurs figurant aux points 3° et 4° du tableau de l'annexe et qu'elles ne sont soumises à aucune des obligations prévues aux chapitres 4 et 5. De même, cette notification précise, le cas échéant, que les entités critiques concernées sont des entités des secteurs figurant au point 8° du tableau de l'annexe et qu'elles ne sont soumises à aucune des obligations prévues aux chapitres 4 et 5, pour les activités qui tombent sous la surveillance de la Commission de surveillance du secteur financier.

(7) Si nécessaire et en tout état de cause au moins tous les quatre ans, les autorités compétentes réexaminent et, s'il y a lieu, mettent à jour la liste des entités critiques recensées et désignées visées au paragraphe 4. Lorsque ces mises à jour entraînent le recensement et la désignation d'entités critiques supplémentaires, les paragraphes 4 à 6 s'appliquent à ces entités critiques supplémentaires. En outre, les autorités compétentes notifient en temps utile les entités qui ne sont plus recensées en tant qu'entités critiques, à la suite d'une telle mise à jour, de ce fait et du fait qu'elles ne sont plus soumises aux obligations prévues au chapitre 4 à compter de la date de réception de cette notification.

Art. 8. L'article 10 et les chapitres 4, 5 et 6 ne s'appliquent pas :

1° aux entités critiques recensées dans les secteurs figurant aux points 3° et 4° du tableau de l'annexe ;
2° aux entités critiques recensées dans le secteur figurant au point 8° du tableau de l'annexe, pour les activités qui tombent sous la surveillance de la Commission de surveillance du secteur financier ;
3° 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 ;
4° aux services du ministre ayant la Défense dans ses attributions ;
5° à l'Armée luxembourgeoise visée par la loi modifiée du 7 août 2023 sur l'organisation de l'Armée luxembourgeoise.

Art. 9. (1) Les autorités compétentes aident les entités critiques à renforcer leur résilience.

(2) Les autorités compétentes coopèrent et échangent des informations et des bonnes pratiques avec les entités critiques des secteurs figurant à l'annexe.

Art. 10. Chaque fois que cela est approprié, l'autorité compétente se consulte avec les autorités compétentes des autres États membres de l'Union européenne au sujet des entités critiques aux fins d'assurer l'application cohérente de la présente loi. Ces consultations ont lieu en particulier au sujet des entités critiques qui :

1° utilisent des infrastructures critiques qui sont physiquement connectées entre deux États membres de l'Union européenne ou plus ;

2° font partie de structures d'entreprise qui sont connectées ou liées à des entités critiques dans d'autres États membres de l'Union européenne ;

3° ont été recensées en tant qu'entités critiques dans un État membre de l'Union européenne et fournissent des services essentiels à ou dans d'autres États membres de l'Union européenne.

Chapitre 4 – Résilience des entités critiques

Art. 11. (1) Sans préjudice de l'article 7, paragraphe 4, alinéa 2, les entités critiques procèdent à une évaluation des risques dans un délai de neuf mois suivant la réception de la notification visée à l'article 7, paragraphe 4, et ensuite, selon les besoins, mais au moins tous les quatre ans, sur la base de l'évaluation des risques visée à l'article 6 et d'autres sources d'informations pertinentes, afin d'évaluer tous les risques pertinents qui pourraient perturber la fourniture de leurs services essentiels, ci-après dénommée « évaluation des risques d'entité critique ».

(2) Les évaluations des risques d'entités critiques rendent compte de tous les risques naturels et d'origine humaine pertinents, susceptibles d'entraîner un incident, y compris ceux qui revêtent un caractère transsectoriel ou transfrontière, des accidents, des catastrophes naturelles, des urgences de santé publique et des menaces hybrides et autres menaces antagonistes, lesquelles comprennent les infractions terroristes prévues par le Code pénal. Une évaluation des risques d'entité critique tient compte de la mesure dans laquelle d'autres secteurs figurant à l'annexe dépendent du service essentiel fourni par l'entité critique et de la mesure dans laquelle cette entité critique dépend des services essentiels fournis par d'autres entités de ces autres secteurs, y compris s'il y a lieu, dans les États membres de l'Union européenne voisins et les pays tiers.

Lorsqu'une entité critique a réalisé d'autres évaluations des risques ou établi des documents en vertu d'obligations prévues dans d'autres actes juridiques qui sont pertinents pour son évaluation des risques d'entité critique, elle peut utiliser ces évaluations et documents pour

satisfaire aux exigences énoncées dans le présent article. Dans l'exercice de ses fonctions de supervision, l'autorité compétente peut déclarer qu'une évaluation des risques existante réalisée par une entité critique qui porte sur les risques et le degré de dépendance visés à l'alinéa 1er respecte, en tout ou en partie, les obligations prévues par le présent article.

Art. 12. (1) Les entités critiques prennent des mesures techniques, des mesures de sécurité et des mesures organisationnelles appropriées et proportionnées pour garantir leur résilience, sur la base des informations pertinentes fournies par l'autorité compétente concernant l'évaluation des risques visée à l'article 6 et les résultats de l'évaluation des risques d'entité critique, y compris des mesures nécessaires pour :

1° prévenir la survenance d'incidents, en tenant dûment compte de mesures de réduction des risques de catastrophe et d'adaptation au changement climatique ;

2° assurer une protection physique adéquate de leurs locaux et infrastructures critiques ;

3° réagir et résister aux conséquences des incidents et les atténuer, en prenant dûment en considération la mise en œuvre de procédures et protocoles de gestion des risques et des crises et de procédures d'alerte ;

4° se rétablir d'incidents, en prenant dûment en considération des mesures assurant la continuité des activités et la détermination d'autres chaînes d'approvisionnement, afin de reprendre la fourniture du service essentiel ;

5° assurer une gestion adéquate de la sécurité liée au personnel, en prenant dûment en considération des mesures telles que la définition des catégories de personnel qui exercent des fonctions critiques, l'établissement de droits d'accès aux locaux, aux infrastructures critiques et aux informations sensibles, la mise en place de procédures de vérification des antécédents conformément aux articles 13 à 15, la désignation des catégories de personnes tenues de faire l'objet de telles vérifications des antécédents et la définition d'exigences et de qualifications appropriées en matière de formation ;

6° sensibiliser le personnel concerné aux mesures visées aux points 1° à 5°, en tenant dûment compte des séances de formation, du matériel d'information et des exercices.

Aux fins de l'alinéa 1er, point 5°, les entités critiques tiennent compte du personnel des prestataires de services extérieurs lorsqu'ils définissent les catégories de personnel qui exercent des fonctions critiques.

(2) Les entités critiques mettent en place et appliquent un plan de résilience ou un ou plusieurs documents équivalents, qui décrivent les mesures prises en application du paragraphe 1er. Lorsque les entités critiques ont élaboré des documents ou pris des mesures en vertu d'obligations prévues dans d'autres actes juridiques qui sont pertinents pour les mesures visées au paragraphe 1er, elles peuvent utiliser ces documents et mesures pour satisfaire aux exigences énoncées dans le présent article. Dans l'exercice de ses fonctions de supervision, l'autorité compétente peut déclarer que des mesures existantes de renforcement de la résilience prises par une entité critique qui portent, de manière appropriée et proportionnée, sur les mesures techniques, les mesures de sécurité et les mesures organisationnelles visées au paragraphe 1er respectent, en tout ou en partie, les obligations prévues par le présent article.

(3) Chaque entité critique désigne un agent de liaison ou une personne ayant une fonction équivalente en tant que point de contact avec l'autorité compétente.

Art. 13. (1) La Police grand-ducale procède, sur demande de l'entité critique et dans le seul but d'évaluer un risque potentiel pour la sécurité de l'entité concernée, à des vérifications des antécédents des personnes :

1° qui occupent des fonctions sensibles au sein de l'entité critique ou au bénéfice de celle-ci, notamment en ce qui concerne la résilience de l'entité critique ;

2° qui occupent la fonction de responsable du système informatique ou du système de contrôle de l'entité critique ; ou

3° dont le recrutement est envisagé à des postes répondant aux critères énoncés aux points 1° ou 2°.

Par rapport aux données qu'elle traite dans ce contexte, la Police grand-ducale est le responsable du traitement tel que défini par la loi du 1er août 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité.

Préalablement à l'introduction de la demande de vérification des antécédents, les catégories de personnes tenues de faire l'objet d'une vérification des antécédents désignées dans le cadre des mesures prévues à l'article 12, sont approuvées par l'autorité compétente. Une copie de cette approbation est transmise à la Police grand-ducale.

(2) La demande visée au paragraphe 1er contient les éléments suivants :

1° l'identité de la personne visée au paragraphe 1er : noms et prénoms, date et lieu de naissance, résidence, nationalité, numéro d'identification national et numéro de la pièce d'identité ainsi qu'une photographie récente ;

2° la nature du contrat de travail ou de la relation juridique liant la personne visée au paragraphe 1er à l'entité critique ;

3° la déclaration écrite ou électronique de la personne visée au paragraphe 1er, contenant l'autorisation de procéder à une vérification des antécédents ;

4° une liste des lieux de résidence des cinq dernières années et un certificat de résidence datant de moins de trois mois ;

5° un extrait du casier judiciaire des pays où la personne visée au paragraphe 1er a résidé les cinq dernières années ou dont elle a la nationalité, à l'exception du Luxembourg, datant de moins de trois mois ;

6° l'accord de la personne visée au paragraphe 1er, que le bulletin N° 2 du casier judiciaire puisse être délivré directement à la Police grand-ducale ;

7° la signature de la personne visée au paragraphe 1er ;

8° le cachet et la signature de l'entité dont relève la personne visée au paragraphe 1er, précédés d'une attestation de ladite entité certifiant le bien-fondé et les motifs de la demande ;

9° une documentation concernant les emplois et les études au cours des cinq dernières années ;

10° une photocopie de la carte d'identité ou du passeport en cours de validité ;

11° un questionnaire biographique dûment rempli.

La Police grand-ducale, dans le cadre de ses recherches :

1° consulte les fichiers visés à l'article 43, paragraphe 1er, points 1°, 2° et 14° de la loi modifiée du 18 juillet 2018 sur la Police grand-ducale, pour autant que cette consultation soit pertinente quant à la finalité recherchée ;

2° adresse une demande motivée au procureur général d'État en vue de l'obtention d'un extrait du casier judiciaire de l'autorité compétente de l'État membre de l'Union européenne dont la personne a la nationalité ou de l'autorité compétente de l'État membre de l'Union européenne dans lequel la personne a résidé au cours des cinq dernières années si la personne visée à l'article 13, paragraphe 1er, possède la nationalité d'un pays étranger ou réside dans un pays étranger et sous condition de disposer de l'accord écrit ou électronique de cette personne ;

3° consulte tout employeur de la personne concernée ou tout établissement d'éducation fréquenté par la personne concernée afin de vérifier l'authenticité des informations fournies.

(3) La Police grand-ducale procède à la vérification des antécédents sur une période de cinq ans précédant la demande.

Toute demande incomplète est retournée à l'entité critique requérante et non traitée.

(4) Au terme de la vérification, la Police grand-ducale émet, en application de l'alinéa 2, un avis relatif au risque potentiel que la personne visée au paragraphe 1er représente pour la sécurité de l'entité critique.

La personne visée au paragraphe 1er est considérée comme présentant un risque pour la sécurité de l'entité critique s'il est constaté qu'elle a :

1° commis ou tenté de commettre une des infractions contre la sûreté de l'État visées aux articles 101 à 135-17 du Code pénal ;

2° commis ou tenté de commettre une des infractions de faux en écriture et d'usage de faux en écriture visées aux articles 194 à 197 du Code pénal ;

3° commis ou tenté de commettre une des infractions de corruption visées aux articles 246 à 250 du Code pénal ;

4° commis ou tenté de commettre une des infractions d'escroquerie et de tromperie visées aux article 496 à 501 du Code pénal ; ou

5° sciemment fait des fausses déclarations en relation avec la demande de vérification des antécédents.

La Police grand-ducale transmet cet avis motivé au ministre ayant la Protection nationale dans ses attributions, ci-après « ministre ».

Art. 14. (1) Le ministre émet une décision relative au risque potentiel que la personne visée à l'article 13, paragraphe 1er, représente pour la sécurité de l'entité critique, en prenant en considération l'avis de la Police grand-ducale.

(2) Le ministre notifie la décision motivée relative à la vérification des antécédents à la personne visée à l'article 13, paragraphe 1er.

(3) Le ministre transmet la décision à l'entité critique requérante sans lui communiquer les informations personnelles qu'il a reçues dans l'avis de la Police grand-ducale. L'entité critique requérante est tenue de suivre la décision du ministre.

(4) La personne visée à l'article 13, paragraphe 1er, au sujet de laquelle le ministre a constaté, à travers sa décision visée au paragraphe 1er, qu'elle présente un risque pour la sécurité de l'entité critique peut, sur demande écrite et dans un délai de trente jours à partir de la date de notification de la décision, à adresser au ministre, solliciter l'accès au dossier sur lequel est fondée sa décision.

Elle peut, à cette fin, consulter toutes les pièces du dossier constitué par le ministre dans le cadre de la prise de décision relative à la vérification des antécédents.

La demande introduite auprès du ministre n'interrompt pas les délais de recours devant les juridictions administratives.

(5) La décision du ministre visée au paragraphe 1er a une durée de validité de cinq ans. Une demande de renouvellement pour une vérification des antécédents est à introduire par l'entité critique au plus tôt six mois et au plus tard quatre mois avant la fin de validité de la décision du ministre.

La décision de renouvellement de la vérification des antécédents prend effet à la fin de validité de la décision antérieure.

Art. 15. (1) La Police grand-ducale met en place un système informatique centralisé permettant de faciliter la gestion administrative des demandes de vérification des antécédents.

(2) Les données à caractère personnel en relation avec les vérifications des antécédents sont détruites six mois après une décision ayant acquis force de chose décidée ou jugée.

(3) Lors de l'effacement des données à caractère personnel par la Police grand-ducale et dans un but de retraçage et de protection des preuves, une fiche succincte est conservée pendant un délai maximal de cinq ans. Celle-ci contient les informations suivantes :

1° les nom, prénom, date et lieu de naissance, ainsi que le numéro d'identification national et les nationalités de la personne visée à l'article 13, paragraphe 1er ;

2° la mention d'avis « positif » ou « négatif » ;

3° la date d'émission de l'avis.

Art. 16. (1) Les entités critiques notifient sans retard injustifié à l'autorité compétente les incidents qui perturbent ou sont susceptibles de perturber de manière importante la fourniture de services essentiels. Sauf à être dans l'incapacité de le faire pour des raisons opérationnelles, les entités critiques présentent une première notification au plus tard vingt-quatre heures après avoir pris connaissance d'un incident, suivie, s'il y a lieu, d'un rapport détaillé au plus tard un mois après. Afin de déterminer l'importance de la perturbation, les paramètres suivants sont, en particulier, pris en compte :

1° le nombre et la proportion d'utilisateurs affectés par la perturbation ;

2° la durée de la perturbation ;

3° la zone géographique concernée par la perturbation, en tenant compte de son éventuel isolement géographique.

Les paramètres permettant de déterminer l'importance de la perturbation sont précisés par règlement grand-ducal.

(2) Les notifications visées au paragraphe 1er comprennent toutes les informations disponibles nécessaires pour permettre à l'autorité compétente de comprendre la nature, la cause et les conséquences possibles de l'incident, y compris toute information disponible nécessaire pour déterminer tout impact transfrontière de l'incident. Ces notifications n'ont pas pour effet de soumettre les entités critiques à une responsabilité accrue.

(3) Sur la base des informations fournies par une entité critique dans une notification visée au paragraphe 1er, l'autorité compétente, par l'intermédiaire du point de contact unique, informe le point de contact unique des autres États membres de l'Union européenne affectés lorsque l'incident a ou pourrait avoir un impact important sur les entités critiques et sur la continuité de la fourniture de services essentiels à ou dans un ou plusieurs autres États membres de l'Union européenne.

Le point de contact unique qui envoie et reçoit des informations en vertu de l'alinéa 1er traite ces informations de manière à en respecter la confidentialité et à préserver la sécurité et les intérêts commerciaux de l'entité critique concernée.

(4) Dès que possible après la réception d'une notification visée au paragraphe 1er, l'autorité compétente fournit à l'entité critique concernée des informations de suivi pertinentes, y compris des informations qui pourraient aider ladite entité critique à réagir efficacement à l'incident en question. L'autorité compétente informe le public lorsqu'elle estime qu'il serait dans l'intérêt général de le faire.

Chapitre 5 – Entités critiques d'importance européenne particulière

Art. 17. (1) Une entité est considérée comme une entité critique d'importance européenne particulière lorsqu'elle :

1° a été désignée en tant qu'entité critique conformément à l'article 7, paragraphe 1er ;

2° fournit les mêmes services essentiels ou des services essentiels similaires à ou dans six États membres de l'Union européenne ou plus ; et

3° a fait l'objet d'une notification de la part de la Commission européenne, par l'intermédiaire de son autorité compétente, qu'elle est considérée comme une entité critique d'importance européenne particulière.

(2) Les entités critiques d'importance européenne particulière accordent aux missions de conseil organisées par la Commission européenne afin d'évaluer les mesures mises en place par ladite entité pour satisfaire aux obligations qui lui incombent en vertu du chapitre 4, l'accès aux informations, systèmes et installations relatifs à la fourniture de leurs services essentiels nécessaires à l'exécution de la mission de conseil concernée.

Chapitre 6 – Supervision et exécution

Art. 18. (1) Afin d'évaluer le respect des obligations découlant de la présente loi, l'autorité compétente est autorisée à :

1° procéder à des inspections sur place de l'infrastructure critique et des locaux utilisés par l'entité critique pour fournir ses services essentiels afin de s'assurer de la mise en œuvre des mesures prises par les entités critiques conformément à l'article 12 ;

2° procéder à la supervision à distance des mesures prises par les entités critiques conformément à l'article 12 ;

3° ordonner un audit visant à contrôler la mise en œuvre effective des mesures prises par les entités critiques conformément à l'article 12.

Les inspections sur place prévues à l'alinéa 1er, point 1°, se font entre huit heures et dix-sept heures, moyennant préavis d'au moins deux semaines, par un agent du groupe de traitement ou du groupe d'indemnité A1 ou A2 de l'autorité compétente. Ces inspections pourront se dérouler en dehors de cette plage horaire, en cas d'accord de l'entité critique.

Les agents visés à l'alinéa 2 signalent leur présence à l'agent de liaison de l'entité critique ou, le cas échéant, à son remplaçant. Ce dernier peut les accompagner et leur prêter concours, le cas échéant, pour mener à bien les inspections.

L'agent visé à l'alinéa 2 est tenu de dresser un rapport relatif à l'inspection opérée. Une copie de ce rapport est transmise à l'agent de liaison de l'entité critique.

(2) Les entités en vertu de la loi du XXX concernant des mesures destinées à assurer un niveau élevé de cybersécurité désignées en tant qu'entités critiques en vertu de la présente loi sont tenues de fournir à l'autorité compétente, dans un délai raisonnable fixé par celle-ci :

1° les informations nécessaires pour évaluer si les mesures prises par ces entités pour garantir leur résilience satisfont aux exigences énoncées à l'article 12 ;

2° la preuve de la mise en œuvre effective de ces mesures, y compris les résultats d'un audit effectué par un auditeur indépendant et qualifié sélectionné par ladite entité et effectué à ses frais.

Ces données comprennent toutes les informations qui sont nécessaires dans le contexte de la prévention ou de la gestion d'une crise en vertu de la loi modifiée du 23 juillet 2016 portant création d'un Haut-Commissariat à la Protection nationale.

Lorsqu'elle requiert ces informations, l'autorité compétente mentionne la finalité de la demande et précisent les informations exigées.

(3) Sans préjudice de la possibilité d'imposer des sanctions conformément à l'article 19, l'autorité compétente peut, à la suite des mesures de supervision visées au paragraphe 1er ou de l'évaluation des informations visées au paragraphe 2, enjoindre aux entités critiques concernées de prendre les mesures nécessaires et proportionnées pour remédier à toute violation constatée de la présente loi, dans un délai raisonnable fixé par ladite autorité, et de lui fournir des informations sur les mesures prises. Ces injonctions tiennent compte, notamment, de la gravité de la violation.

(4) Lorsque l'autorité compétente évalue le respect par une entité critique de ses obligations en vertu du présent article, elle en informe les autorités compétentes nationales en vertu de la loi du XXX concernant des mesures destinées à assurer un niveau élevé de cybersécurité.

À cette fin, l'autorité compétente demande aux autorités compétentes nationales en vertu de la loi du XXX concernant des mesures destinées à assurer un niveau élevé de cybersécurité d'exercer leurs pouvoirs de supervision et d'exécution à l'égard d'une entité relevant de ladite directive qui a été désignée en tant qu'entité critique en vertu de la présente loi. À cette fin, l'autorité compétente coopère et échange des informations avec les autorités nationales compétentes en vertu de la loi du XXX concernant des mesures destinées à assurer un niveau élevé de cybersécurité.

Art. 19. (1) Lorsque l'autorité compétente constate une violation des obligations prévues par les articles 11, paragraphes 1er et 2, alinéa 1er, 12, paragraphes 1er à 3, 14, paragraphe 3, 16, paragraphes 1er et 2, 17, paragraphe 2, et 18, paragraphe 2, alinéas 1er et 2, elle peut frapper l'entité critique 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 engage une procédure contradictoire dans laquelle l'entité critique concernée a la possibilité de consulter le dossier et de présenter ses observations écrites ou verbales. L'entité critique concernée peut se faire assister ou représenter par une personne de son choix. À l'issue de la procédure contradictoire, l'autorité compétente peut prononcer à l'encontre de l'entité critique concernée une ou plusieurs des sanctions visées au paragraphe 1er.

(3) Les décisions prises par l'autorité compétente à l'issue de la procédure contradictoire sont motivées et notifiées à l'entité critique 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'autorité compétente moyennant la transmission d'une copie des décisions de fixation. Le recouvrement est poursuivi comme en matière d'enregistrement.

Chapitre 7 – Dispositions modificatives

Art. 20. La loi modifiée du 23 juillet 2016 portant création d'un Haut-Commissariat à la Protection nationale est modifiée comme suit :

1° A l'article 1er, alinéa 1er, les termes « infrastructures critiques » sont remplacés par ceux de « entités critiques » ;

2° L'article 2, point 4°, est remplacé par le texte suivant :

« 4. « entité critique » : une entité au sens de la loi du XXX sur la résilience des entités critiques ; » ;

3° L'article 3 est modifié comme suit :

a) Le paragraphe 1er, lettre b), point 3°, est remplacé par le texte suivant :

« 3. de veiller à l'exécution des mesures relatives à la résilience des entités critiques en application de la loi du XXX sur la résilience des entités critiques ; » ;

b) Aux paragraphes 1*ter*, lettre g), 1*quater*, lettres a) et b), et 3, première phrase, les termes « infrastructures critiques » sont remplacés par ceux de « entités critiques » ;

4° L'intitulé du chapitre 4 est remplacé par l'intitulé suivant :

« Chapitre 4 – La protection des entités critiques » ;

5° Les articles 4 à 8 sont abrogés ;

6° A l'article 9, alinéa 1er, les termes « infrastructure critique » sont remplacés par ceux de « entité critique » et le terme « infrastructure » est remplacé par celui de « entité ».

Chapitre 8 – Intitulé de citation

Art. 21. La référence à la présente loi se fait sous la forme suivante : « loi du XXX sur la résilience des entités critiques ».

ANNEXE

Secteurs, sous-secteurs et catégories d'entités

Secteurs	Sous-secteurs	Catégories d'entités
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 assurent la fonction de « fourniture » au sens de l'article 1er, point 21°, de la même 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, qui fournissent 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

	b) Réseaux de chaleur et de froid	- Opérateurs de réseaux de chaleur ou de réseau 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 de 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 de 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 de 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 de 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) nº 2320/2002, tel que modifié, utilisés à des fins commerciales
		- Entités gestionnaires d'aéroports au sens de l'article 2, point 1°, de 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 réseaux central énumérés à l'annexe II, section 2, du règlement (UE) n° 1315/2013 du Parlement européen et du Conseil du 11 décembre 2013 sur les orientations de l'Union pour le développement du réseau transeuropéen de transport et abrogeant la décision nº 661/2010/UE, tel que modifié, et entités exploitant les installations annexes se trouvant dans les aéroports
		- Services du contrôle de la circulation aérienne assurant les 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 et exploitants d'installations de services 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 visé 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 ateliers 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 des 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
	e) Transports publics	- Opérateurs de services publics au sens de l'article 2, lettre d), du règlement (CE) nº 1370/2007 du Parlement européen et du Conseil du 23 octobre 2007 relatif aux services publics de transport de voyageurs par chemin de fer et par route, et abrogeant les règlements (CEE) n° 1191/69 et (CEE) n° 1107/70 du Conseil, tel que modifié
3. Secteur bancaire		- Établissements de crédit au sens de l'article 4, point 1°, du règlement (UE) nº 575/2013 du Parlement européen et du Conseil du 26 juin 2013 concernant les exigences prudentielles applicables aux établissements de crédit et aux entreprises d'investissement et modifiant le règlement (UE) n° 648/2012, tel que modifié
		- Exploitants de plates-formes de négociation au sens de l'article 1er,

4. Infrastructures des marchés financiers		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'UE 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
		- Entités titulaires d'une autorisation de distribution au sens de l'article 4 de la loi modifiée du 6 janvier 1995 relative à la distribution en gros des médicaments
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, 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 résiduaires		- Entreprises collectant, évacuant ou traitant les eaux urbaines résiduaires, des eaux ménagères usées ou des 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. Infrastructures numériques		- Fournisseurs de points d'échange internet au sens de l'article 2, point 17°, de la loi du XXX concernant des mesures destinées à assurer un niveau élevé de cybersécurité
		- Fournisseurs de services DNS au sens de l'article 2, point 19°, de la loi du XXX concernant des mesures destinées à assurer un niveau élevé de cybersécurité, à l'exclusion des opérateurs de serveurs racines de noms de domaines
		- Registres de noms de domaines de premier niveau au sens de l'article 2, point 20°, de la loi du XXX concernant des mesures destinées à assurer un niveau élevé de cybersécurité

		- Fournisseurs de services d'informatique en nuage au sens de l'article 2, point 29°, de la loi du XXX concernant des mesures destinées à assurer un niveau élevé de cybersécurité
		- Fournisseurs de services de centre de données au sens de l'article 2, point 30°, de la loi du XXX concernant des mesures destinées à assurer un niveau élevé de cybersécurité
		- Fournisseurs de réseaux de diffusion de contenu au sens de l'article 2, point 31°, de la loi du XXX concernant des mesures destinées à assurer un niveau élevé de cybersécurité
		- Prestataires de services de confiance au sens de l'article 3, point 19°, du règlement (UE) nº 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE
		- Fournisseurs de réseaux de communications électroniques publics au sens de l'article 2, point 8°, de la loi du 17 décembre 2021 sur les réseaux et les services de communications électroniques
		- Fournisseurs de services 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 dans la mesure où leurs services sont accessibles au public
9. Administration publique		- Entité de l'administration publique telle que définie à l'article 2, point 9°
10. Espace		- Exploitants d'infrastructures au sol, détenues, gérées et exploitées par des États membres ou par des parties privées, qui soutiennent la fourniture de services spatiaux, à l'exclusion des fournisseurs de réseaux de communications électroniques publics au sens de l'article 2, point 8°, de la loi du 17 décembre 2021 sur les réseaux et les services de communications
11. Production, transformation et		- Entreprises du secteur alimentaire au sens de l'article 3, point 2°, du

	distribution de denrées alimentaires		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 exclusivement des activités de logistique et de distribution en gros ainsi que de production et de transformation industrielles à grande échelle
12.	Gestion des déchets		- Entreprise impliquée dans la gestion des déchets au sens de l'article 4, point 22°, de la loi modifiée du 21 mars 2012 relative aux déchets

Luxembourg, le 13 avril 2026

Le Président-Rapporteur,
Laurent Zeimet