

Commission des Institutions

Procès-verbal de la réunion du 09 décembre 2024

Ordre du jour :

1. Approbation du projet de procès-verbal de la réunion du 11 novembre 2024
2. 8364 Projet de loi concernant des mesures destinées à assurer un niveau élevé de cybersécurité et portant modification de :
1° la loi modifiée du 14 août 2000 relative au commerce électronique ;
2° la loi modifiée du 23 juillet 2016 portant création d'un Haut-Commissariat à la Protection nationale ;
3° la loi du 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 ;
4° la loi du 17 décembre 2021 sur les réseaux et les services de communications électroniques
 - Désignation d'un Rapporteur
 - Présentation du projet de loi
 - Examen de l'avis du Conseil d'Etat
3. 8398 Proposition de loi modifiant l'article 126 de la loi électorale modifiée du 18 février 2003
 - Rapporteur : Monsieur Gilles Baum
 - Examen de l'avis du Conseil d'Etat
 - Examen de la prise de position du Gouvernement
4. Divers

*

Présents : 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. Laurent Zeimet

M. Alex Donnersbach remplaçant M. Michel Wolter
M. Ben Polidori, observateur

Mme Anne Greiveldinger, du Ministère d'Etat
M. Guy Bley, Haut-Commissaire à la Protection nationale
M. Frank Lieser, Mme Elisabeth Wirion, du Haut-Commissariat à la Protection nationale

Mme Carole Closener, de l'Administration parlementaire

Excusés : M. Charles Weiler, M. Michel Wolter
M. Sven Clement, observateur délégué

*

Présidence : M. Laurent Zeimet, Président de la Commission

*

1. Approbation du projet de procès-verbal de la réunion du 11 novembre 2024

Le projet de procès-verbal de la réunion du 11 novembre 2024 est approuvé.

- 2. 8364 Projet de loi concernant des mesures destinées à assurer un niveau élevé de cybersécurité et portant modification de :**
1° la loi modifiée du 14 août 2000 relative au commerce électronique ;
2° la loi modifiée du 23 juillet 2016 portant création d'un Haut-Commissariat à la Protection nationale ;
3° la loi du 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 ;
4° la loi du 17 décembre 2021 sur les réseaux et les services de communications électroniques

Désignation d'un rapporteur

M. Laurent Zeimet est désigné rapporteur du projet de loi.

Présentation du projet de loi

Les représentants du HCPN exposent les grandes lignes du projet de loi, telles que reprises par la présentation PowerPoint annexée.

Examen de l'avis du Conseil d'Etat

Dans son avis du 8 octobre 2024, le Conseil d'Etat note qu'une grande partie des dispositions transposent fidèlement la directive NIS 2.

Outre 10 oppositions formelles, il émet une série de remarques d'ordre légistique.

Enfin, il demande de veiller à ce que la loi transposant la directive 2022/2557 (« directive CER »), objet du projet de loi n°8307, entre en vigueur au plus tard concomitamment avec la loi en projet.

Pour les détails de l'avis du Conseil d'Etat, il est prié de se référer au document parlementaire afférent.

Examen de l'avis de la Chambre de Commerce

La Chambre de Commerce accueille favorablement le projet de loi qui vise à contribuer à assurer un niveau élevé de cybersécurité, à mettre en place une stratégie au niveau national et à renforcer la coopération et l'échange d'informations dans le domaine de la cybersécurité au niveau européen.

Elle note que le projet de loi s'inscrit dans le respect d'une transposition fidèle de la Directive NIS 2.

Certains éléments relatifs à la mise en œuvre de la future loi mériteraient néanmoins d'être précisés dans un souci de sécurité juridique et de proportionnalité pour les opérateurs visés par les obligations qui y sont prévues.

- Il en est ainsi des délais dans lesquels les entités vont devoir s'enregistrer auprès des autorités compétentes (art. 11, §4).
- En ce qui concerne la sécurité de la chaîne d'approvisionnement, elle demande de préciser si tous les fournisseurs et prestataires de services d'une entité doivent être pris en compte ainsi que de fournir des orientations sur le niveau de cybersécurité attendu et le niveau de vérification adéquat à mettre en place par les entités (art. 12, §2, pt. 4).
- En outre, elle suggère un standard de formation pour les membres des organes de direction (art. 13, §2).
- Par ailleurs, elle propose de préciser la gradation des sanctions (art. 22, 23, 25).

La Chambre de Commerce approuve le projet de loi sous avis, sous réserve de la prise en compte de ses remarques.

Pour les détails de l'avis de la Chambre de Commerce, il est prié de se référer au document parlementaire afférent.

Echange de vues

De l'échange de vues subséquent, il y a lieu de retenir les éléments suivants :

- Avec la directive NIS 2, les entités doivent s'enregistrer elles-mêmes.
- Dans la première version de NIS, les Etats membres désignaient des OSE (Opérateurs de Services Essentiels) et des FSN (Fournisseurs de Services Numériques), qui avaient l'obligation de déclarer leurs systèmes d'information auprès des agences gouvernementales compétentes. La conséquence était que le traitement était disparate à travers l'Union européenne. Avec la directive NIS 2, l'approche est simplifiée : si une entreprise répond aux critères, elle est incluse. Il n'y a ici plus besoin de déclaration spécifique.
- En pratique, toutes les administrations publiques sont concernées.
- Les communes sont incluses étant donné leur rôle de fournisseur et distributeur d'eau.
- Le SYVICOL devra être saisi pour avis.
- L'ILR a organisé des sessions d'information sur la directive NIS 2.

- Le délai de transposition était fixé au 17 octobre 2024. Parmi les Etats membres, les avancées sont assez hétérogènes dans le processus de transposition. Seule une minorité d'Etats a su transposer dans les délais.

3. 8398 Proposition de loi modifiant l'article 126 de la loi électorale modifiée du 18 février 2003

Le rapporteur de la proposition de loi, M. Gilles Baum, présente les grandes lignes de l'avis du Conseil d'Etat et de la prise de position du Gouvernement (pour le détail desquels il est prié de se référer aux documents parlementaires afférents).

Examen de l'avis du Conseil d'Etat

Dans son avis du 26 novembre 2024, le Conseil d'Etat attire l'attention sur le fait que, malgré les affirmations des auteurs du texte, la suppression du délai dans lequel un licenciement des collaborateurs doit avoir lieu pour que le député puisse avoir un remboursement de la part de la Chambre des Députés risque d'aggraver la dépense publique. Selon la Haute Corporation, l'engagement du collaborateur pourrait se prolonger dans le temps, ayant potentiellement pour conséquence une augmentation tant de l'indemnité de préavis que de l'indemnité de départ, toutes les deux en fonction de l'ancienneté du salarié.

Le Conseil d'Etat propose de limiter le remboursement aux indemnités de préavis et de départ calculées sur la base de l'ancienneté de service du collaborateur au moment où le mandat du député employeur a pris fin.

En ce qui concerne le report des effets de la modification au jour des élections législatives du 8 octobre 2023, le Conseil d'Etat considère que la rétroactivité ne heurte ni les droits de tiers, ni les principes de sécurité juridique.

Examen de la prise de position du Gouvernement

Dans sa prise de position du 12 septembre 2024, le Gouvernement note que la modification proposée vise à remédier à une situation qui se révèle désavantageuse, non seulement pour les députés mais également pour les collaborateurs qui peuvent se voir licenciés dans la précipitation. Le Gouvernement remarque que la suppression de la condition temporelle permet aux députés non réélus d'organiser une éventuelle reprise des salariés par leurs successeurs avant de prendre une décision de licencier ou non.

Eu égard aux points susmentionnés, le Gouvernement approuve la proposition de loi.

*

M. le rapporteur propose de finaliser son projet de rapport en vue d'une adoption qui pourrait avoir lieu dès le mois de janvier.

4. Divers

La prochaine réunion aura lieu le 13 janvier 2025 à 10h00.

Luxembourg, le 09 décembre 2024

Procès-verbal approuvé et certifié exact

Annexe : PL n° 8364 - Présentation PowerPoint



Projet de loi n° 8364 concernant des mesures destinées à assurer un niveau élevé de cybersécurité

Transposition de la directive « NIS 2 »

Commission des Institutions – 9 décembre 2024



LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Haut-Commissariat
à la protection nationale



- Directive 2022/2555 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union (ci-après « **directive NIS 2** », successeur de la *directive on security of network and information systems* – NIS 1)

- **But ?** Renforcer la cybersécurité au niveau européen

- **Comment ?**
 - Obligations en matière de sécurité numérique imposées aux **entités essentielles** et **entités importantes**
 - Obligation pour les EM de mettre en place une **stratégie nationale en matière de cybersécurité**
 - Renforcement de la **coopération européenne** en matière de cybersécurité



- **Qui ? Une grande entreprise** qui :
- occupe au moins 250 personnes ou
 - dont le chiffre d'affaires annuel excède 50 millions d'euros ou
 - dont le total du bilan annuel excède 43 millions d'euros

+ active dans un des **secteurs hautement critiques** (*Annexe I*) :

- Énergie
- Transport
- Secteur bancaire
- Infrastructures des marchés financiers
- Santé
- Eau potable
- Eaux usées
- Infrastructure numérique
- Gestion des services TIC
- Administration publique
- Espace



- **Qui ?** Une **moyenne entreprise** qui :
 - occupe au moins 50 personnes ou
 - a un chiffre d'affaires annuel ou
 - un total du bilan annuel d'au moins 10 millions d'euros, sans dépasser les seuils qui la qualifieraient de grande entreprise

+ active dans un des **secteurs hautement critiques** (*Annexe I*)

et



➤ **Qui ?** Une **grande** ou **moyenne entreprise** active dans les **autres secteurs critiques** (*Annexe II*) :

- Services postaux et d'expédition
- Gestion des déchets
- Fabrication, production et distribution de produits chimiques
- Production, transformation et distribution des denrées alimentaires
- Fournisseurs numériques
- Recherche
- Fabrication



➤ ***Sont toujours considérées comme entités essentielles :***

- Entités identifiées comme **critiques** en vertu du projet de loi « CER »
- **Prestataires de services de confiance qualifiés, registres de noms de domaine de premier niveau et fournisseurs de services DNS**, quelle que soit leur taille
- **Fournisseurs de réseaux publics de communications électroniques publics et services de communications électroniques accessibles au public** qui constituent des moyennes entreprises
- Entités de l'**administration publique**
- Toute autre entité d'un type visé à l'annexe I ou II qui est **identifié par l'autorité compétente** en tant qu'entité essentielle
- **Opérateurs de services essentiels** sous NIS 1



➤ Quelles obligations ?

- Obligation de mettre en place des **mesures de gestion des risques** en matière de cybersécurité
- Obligation de **notification** de tout incident important

➤ Différence dans la rigueur du contrôle



➤ Qui ?

ILR :

- Tous les secteurs des annexes I et II, à l'exception des secteurs tombant sous la compétence de la CSSF

CSSF :

- Secteur bancaire
- Infrastructures des marchés financiers
- Gestion des services TIC *pour les activités qui tombent sous sa surveillance*
- Infrastructures numériques *pour les activités qui tombent sous sa surveillance*

➤ Missions ?

- **Supervision** et mise en œuvre de la loi
- Pouvoirs d'**exécution** et de **sanction**
- Coordination, **coopération** et échange d'informations



➤ Qui ? HCPN

➤ Missions ?

- Assurer la **coopération transfrontière** entre :
 - autorités compétentes LU + autorités compétentes d'autres EM
 - autorités compétentes LU + institutions UE

- Garantir la **coopération intersectorielle** avec les autres autorités compétentes nationales



➤ Qui ? HCPN

➤ Missions ?

- Adopter un **plan national de réaction** aux crises et incidents de cybersécurité majeurs
- Représenter LU au sein du réseau européen pour la préparation et la gestion des crises cyber (« **EU-CyCLONe** »).



Centres de réponse aux incidents de sécurité informatique (CSIRT)



➤ Qui ?

- **GOVCERT.LU** pour les administrations et services de l'État, les établissements publics et les entités critiques
- **CIRCL** pour tous les autres

➤ Missions ?

- Prévenir et détecter les incidents et les risques, y réagir et en atténuer l'impact



Stratégie nationale en matière de cybersécurité



- Qui ? HCPN
- **Remplace** la stratégie nationale en matière de sécurité des réseaux et des systèmes d'information instaurée par la directive NIS 1
- Détermine les **objectifs** stratégiques, les **ressources** nécessaires pour atteindre ces objectifs ainsi que les **mesures** politiques et réglementaires appropriées



- La quasi-totalité du texte fait preuve d'une transposition fidèle de la directive
- 10 oppositions formelles
- Remarques d'ordre légistique
- Demande de veiller à ce que la loi transposant la directive 2022/2557 (« directive CER ») entre en vigueur au plus tard concomitamment avec la loi en projet



1. Article 1^{er}, §7

- *Les autorités compétentes visées à l'article 3 déterminent, par voie de règlement ou de circulaire et conformément aux lignes directrices adoptées par la Commission européenne et clarifiant l'application des points 1° et 2°, les actes juridiques sectoriels de l'Union européenne ayant un effet au moins équivalent à la présente loi.*
- Opposition formelle : Le Conseil d'État doit s'opposer formellement à l'alinéa 3 pour **transposition incorrecte** de la directive. Il est proposé aux auteurs soit de supprimer l'alinéa en question soit de le remplacer par une disposition prévoyant la diffusion par les autorités compétentes à l'attention des entités concernées d'une simple information sur le contenu des lignes directrices de la Commission européenne prises sur la base de l'article 4, paragraphe 3, de la directive NIS2.



2. Article 8 <-> Article 11, §1 de la directive NIS 2

➤ *Les CSIRT satisfont aux exigences suivantes:*

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

b) les locaux des CSIRT et les systèmes d'information utilisés se trouvent sur des sites sécurisés;

c) les CSIRT sont dotés d'un système approprié de gestion et de routage des demandes afin, notamment, de faciliter les transferts effectifs et efficaces;

d) les CSIRT garantissent la confidentialité et la fiabilité de leurs opérations;

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

f) les CSIRT sont dotés de systèmes redondants et d'un espace de travail de secours pour assurer la continuité de leurs services.

Les CSIRT peuvent participer à des réseaux de coopération internationale.

➤ Opposition formelle : Le Conseil d'État estime que ces dispositions doivent figurer dans la loi et s'oppose formellement à l'article sous revue pour **transposition incomplète** de la directive.



3. Article 8, §1, al.1, pt. 3°

- *Les CSIRT assument les tâches suivantes : (...) 3° réagir aux incidents et apporter une assistance , à leur demande, aux entités essentielles et importantes concernées ; (...)*
- Opposition formelle : La directive vise la réaction aux incidents et l'assistance aux entités essentielles et importantes concernées « le cas échéant », tandis que le projet de loi vise la réaction aux incidents et l'assistance aux entités essentielles et importantes concernées « à leur demande ». Le Conseil d'État doit dès lors s'opposer formellement à la disposition sous revue pour **transposition incorrecte** de la directive.



4. Article 11, §4, al.3

- *Les autorités compétentes mettent en place un mécanisme national par lequel les entités visées au paragraphe 3 sont dans l'obligation de s'enregistrer elles-mêmes. L'autorité compétente concernée confirme à ces entités concernées leur désignation en tant qu'entité essentielle ou importante.*
- Opposition formelle : Le Conseil d'État s'interroge sur l'articulation entre le §4, al. 3, et le §3. Il s'en dégage l'impression que les auteurs du texte entendent faire de l'enregistrement l'événement déclencheur de l'établissement des listes d'entités essentielles et importantes. Laisser ainsi l'entière initiative aux entités alors qu'aux termes de la directive ce sont les autorités qui doivent établir lesdites listes n'est cependant pas conforme à la norme européenne. Le Conseil d'État s'oppose formellement au libellé du paragraphe 4, alinéa 3, de l'article sous revue, qui est source **d'insécurité juridique**.



5. Article 16, §3

- *En l'absence d'un représentant dans l'Union européenne désigné en vertu du présent paragraphe et si l'entité fournit des services au Luxembourg, l'État luxembourgeois peut intenter une action en justice contre l'entité pour violation de la présente loi.*
- Opposition formelle : Aucune précision quant à l'action à intenter, la juridiction compétente et la procédure applicable. Le Conseil d'État s'oppose formellement à l'article 16, paragraphe 3, pour **transposition incorrecte** de la directive.



6. Article 18, §6

- *Les registres des noms de domaine de premier niveau et les entités fournissant des services d'enregistrement de noms de domaine coopèrent entre eux.*
- Opposition formelle : Le Conseil d'État comprend que la coopération visée par la directive a comme objectif l'échange des données d'enregistrement de noms de domaine. Il demande, sous peine d'opposition formelle pour **transposition incomplète** de la directive, de compléter le §6 par le ou les objectifs de la coopération visée.



7. Article 22, §4, pt. 9°

- *Les autorités compétentes, lorsqu'elles exercent leurs pouvoirs d'exécution à l'égard d'entités essentielles, ont le pouvoir : (...) 9° d'imposer ou de demander aux organes compétents ou aux juridictions d'imposer une amende administrative en vertu de l'article 26 en plus de l'une ou l'autre des mesures visées aux points 1° à 8° du présent paragraphe.*
- Opposition formelle : Le texte laisse subsister une insécurité juridique quant à la nature de l'organe compétent ou de la juridiction en charge d'exercer les pouvoirs décrits sous ce point. Le Conseil d'État doit s'opposer formellement au texte sous revue pour **insécurité juridique** et **non-respect des exigences européennes** en matière de transposition des directives.



8. Article 22, §5, al.1, pt. 1° + 2°

- (...) Si la mesure demandée n'est pas prise dans le délai imparti, les autorités compétentes ont le pouvoir :
 - 1° de suspendre temporairement ou de demander à un organisme de certification ou d'autorisation, ou à une juridiction, de suspendre temporairement une certification ou une autorisation concernant tout ou partie des services pertinents fournis ou des activités pertinentes menées par l'entité essentielle ;
 - 2° de demander aux organes compétents ou aux juridictions compétentes d'interdire temporairement à toute personne physique exerçant des responsabilités dirigeantes à un niveau de directeur général ou de représentant légal dans l'entité essentielle d'exercer des responsabilités dirigeantes dans cette entité.

- Opposition formelle : Sous peine d'opposition formelle pour **insécurité juridique** et **non-respect des exigences européennes** en matière de transposition des directives, le Conseil d'État demande de reformuler les points 1° et 2° du paragraphe en question avec la spécificité, la précision et la clarté requises.



9. Article 23, §4, pt. 8°

- *Les autorités compétentes, lorsqu'elles exercent leurs pouvoirs d'exécution à l'égard d'entités importantes, ont le pouvoir : (...) 8° d'imposer ou de demander aux organes compétents ou aux juridictions compétentes d'imposer une amende administrative en vertu de l'article 26 en plus de l'une ou l'autre des mesures visées aux points 1° à 7°.*
- Opposition formelle : Le Conseil d'État doit s'y opposer formellement pour les mêmes raisons que celles évoquées à l'endroit de l'article 22, paragraphe 4, point 9°, pour **insécurité juridique** et **non-respect des exigences européennes** en matière de transposition des directives.



10. Article 26, §4

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

Article 26, §5

- *Lorsqu'elles violent l'article 12 ou 14, les entités importantes sont soumises, conformément aux paragraphes 2 et 3, à des amendes administratives d'un montant maximal s'élevant à au moins 7 000 000 EUR ou à au moins 1,4 % du chiffre d'affaires annuel mondial total de l'exercice précédent de l'entreprise à laquelle l'entité importante appartient, le montant le plus élevé étant retenu.*



Article 26, §4 + §5

- Opposition formelle : Il appartient aux États membres de fixer une fourchette précise pour ces amendes dont le montant maximal est supérieur ou égal au montant prévu par la directive européenne. Les textes des paragraphes 4 et 5 sont ainsi incohérents, de sorte que le Conseil d'État doit s'y opposer formellement pour **contrariété au principe de légalité des peines** prévu à l'article 19 de la Constitution.



- Accueille favorablement le projet de loi
- Transposition fidèle de la directive NIS 2
- Certains éléments relatifs à la mise en œuvre de la future loi mériteraient d'être précisés
- Approuve le projet de loi, sous réserve de la prise en compte de ses remarques



➤ Résumé :

- Absence de précisions quant aux **délais** endéans lesquels les entités vont devoir **s'enregistrer** auprès des autorités compétentes (art. 11, §4)
- En ce qui concerne la **sécurité de la chaîne d'approvisionnement**, préciser si tous les fournisseurs et prestataires de services d'une entité doivent être pris en compte + fournir des orientations sur le niveau de cybersécurité attendu + niveau de vérification adéquat à mettre en place par les entités (art. 12, §2, pt. 4)
- Suggère un **standard de formation** pour les membres des organes de direction (art. 13, §2)
- Propose de préciser la **gradation des sanctions** (art. 22, 23, 25)



**Nous vous remercions pour votre
attention!**

Questions?



LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Haut-Commissariat
à la protection nationale