

N° 8740²

CHAMBRE DES DÉPUTÉS

PROJET DE LOI

portant mise en œuvre du règlement (UE) 2019/881 en ce qui concerne les services de sécurité gérés et portant modification de la loi du 20 décembre 2024 portant sur certaines modalités d'application et les sanctions du règlement (UE) n° 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) n° 526/2013 (règlement sur la cybersécurité) et portant modification de la loi modifiée du 4 juillet 2014 portant réorganisation de l'ILNAS

* * *

AVIS DE LA CHAMBRE DE COMMERCE

(25.6.2026)

Le projet de loi sous avis (ci-après le « Projet ») a pour objet de mettre en œuvre le règlement (UE) 2025/37 du Parlement européen et du Conseil du 19 décembre 2024, qui modifie le règlement (UE) 2019/881 (ci-après le « Cybersecurity Act »).

Le Cybersecurity Act élargit le champ d'application du règlement (UE) 2019/881 précité qui établit au niveau européen un cadre de certification de cybersécurité visant, d'une part, à garantir un niveau élevé de sécurité pour les produits, services et processus des technologies de l'information et de la communication (TIC) et, d'autre part, à renforcer la confiance dans le marché intérieur numérique. Ainsi, le Cybersecurity Act ne couvre plus uniquement les produits, services et processus TIC, mais inclut désormais également les services de sécurité gérés. Ces derniers consistent « à externaliser tout ou partie de la gestion de la cybersécurité à un fournisseur spécialisé (« Managed Security Service Provider » ou MSSP), chargé de surveiller, gérer et améliorer la sécurité informatique de ses clients ».

Le Projet adapte en conséquence le droit national en modifiant la loi du 20 décembre 2024¹, laquelle organise au Luxembourg le cadre d'application du « Cybersecurity Act », notamment en matière de certification de cybersécurité, d'identification des acteurs concernés, de leurs obligations ainsi que des sanctions applicables en cas de non-respect.

¹ La loi du 20 décembre 2024 portant sur certaines modalités d'application et les sanctions du règlement (UE) n° 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) n° 526/2013 (règlement sur la cybersécurité) et portant modification de la loi modifiée du 4 juillet 2014 portant réorganisation de l'ILNAS

En bref

- La Chambre de Commerce soutient l'adaptation du cadre national de cybersécurité afin d'y intégrer les services de sécurité gérés, en cohérence avec l'évolution du cadre européen.
- Elle regrette toutefois le manque de précision quant au périmètre exact des services de sécurité gérés concernés et recommande d'apporter des clarifications afin de garantir la sécurité juridique des acteurs.
- Elle insiste sur la nécessité d'assurer une mise en œuvre proportionnée, notamment pour les PME, afin d'éviter une charge administrative et financière excessive susceptible de freiner l'innovation.
- Elle appelle à veiller à une articulation cohérente avec les autres cadres réglementaires européens, en particulier la directive NIS2, afin d'éviter tout chevauchement ou duplication des obligations.
- Elle attire l'attention sur le rôle accru de l'Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services (ILNAS) et souligne l'importance de lui garantir des ressources adéquates ainsi qu'un accompagnement dans la montée en compétence.
- La Chambre de Commerce est en mesure d'approuver le projet de loi sous avis, sous réserve de la prise en compte de ses observations.

*

CONSIDÉRATIONS GÉNÉRALES

Le Projet s'inscrit dans un contexte de renforcement du cadre européen de cybersécurité, marqué par une multiplication des menaces et un recours croissant à l'externalisation des fonctions de sécurité informatique.

Dans ce contexte, les services de sécurité gérés jouent un rôle désormais central dans la prévention, la détection et la gestion des incidents de cybersécurité, en particulier pour les entreprises ne disposant pas de ressources internes suffisantes. Leur intégration dans le cadre européen de certification vise à renforcer la fiabilité, la transparence et la comparabilité des prestations offertes sur le marché.

La Chambre de Commerce soutient pleinement cet objectif, qui contribue à renforcer la confiance dans l'économie numérique et à améliorer le fonctionnement du marché intérieur.

Elle souligne toutefois que les services de sécurité gérés, bien qu'inscrits dans la continuité des services TIC, occupent une fonction particulièrement critique dans la gestion des risques de cybersécurité. Leur forte dépendance à l'expertise humaine et à des processus évolutifs appelle, dès lors, une attention particulière afin de garantir un encadrement proportionné, qui ne freine ni l'innovation ni la capacité des acteurs à opérer efficacement.

Par ailleurs, la Chambre de Commerce rappelle que les acteurs concernés sont déjà soumis à plusieurs cadres réglementaires européens, notamment la directive NIS² – transposée en droit luxembourgeois par la loi du 5 mai 2026 concernant des mesures destinées à assurer un niveau élevé de cybersécurité, qui impose des exigences renforcées en matière de gestion des risques de cybersécurité, y compris vis-à-vis des prestataires externes. Dans ce contexte, les services de sécurité gérés peuvent constituer un levier important pour les entreprises souhaitant répondre à ces obligations. Il apparaît dès lors essentiel d'assurer une cohérence d'ensemble entre ces différents cadres afin d'éviter toute complexité excessive.

*

² Lien vers la directive NIS2

COMMENTAIRE DES ARTICLES

Concernant l'article unique du Projet

L'article unique du Projet vise à modifier la loi du 20 décembre 2024 précitée afin d'étendre explicitement son champ d'application aux services de sécurité gérés.

La Chambre de Commerce comprend la logique d'alignement avec le Cybersecurity Act, qui impose d'intégrer ces services dans le cadre de certification existant. Elle relève toutefois que cette extension est opérée de manière essentiellement formelle, par l'ajout des termes « *services de sécurité gérés* » dans plusieurs dispositions, sans que soient précisées les modalités d'application concrètes.

Dans ce contexte, la Chambre de Commerce formule les observations suivantes :

- elle recommande de clarifier le périmètre exact des services de sécurité gérés, notamment au regard de la diversité des prestations existantes (ex : surveillance, réponse aux incidents, tests d'intrusion, audit, conseil, etc.).
- elle souligne l'importance de garantir une mise en œuvre proportionnée, en particulier pour les PME et les acteurs émergents du secteur, afin de ne pas freiner l'innovation ni l'entrée sur le marché.
- elle insiste sur la nécessité de veiller à une coordination avec les autres obligations réglementaires européennes, afin d'éviter des redondances et de limiter la charge administrative.
- elle attire également l'attention sur le rôle central de l'Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services (ILNAS), en tant qu'autorité nationale de certification de cybersécurité chargée de la supervision, de la certification et du contrôle du respect du cadre applicable. L'extension de ses missions aux services de sécurité gérés nécessite de lui assurer des ressources adéquates ainsi qu'un accompagnement dans la montée en compétence.

La Chambre de Commerce soutient l'objectif du Projet visant à adapter le cadre national de cybersécurité aux évolutions du droit européen et à renforcer la confiance dans les services de sécurité gérés. Elle insiste néanmoins sur le fait que la réussite de cet objectif dépendra de la mise en œuvre effective d'un cadre clair, cohérent et proportionné, garantissant à la fois un haut niveau de cybersécurité et la compétitivité des entreprises.

*

Après consultation de ses ressortissants, la Chambre de Commerce est en mesure d'approuver le projet de loi sous avis, sous réserve de la prise en compte de ses observations.

