CHAMBER OF COMMERCE LUXEMBOURG
POWERING BUSINESS

Luxembourg, le 1er août 2023

Objet : Projet de loi n°8132[1] 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 et portant modification de la loi modifiée du 4 juillet 2014 portant réorganisation de l'ILNAS. (6270NHO/GKA)

Saisine : Ministre de l'Economie
(21 décembre 2022)

Avis de la Chambre de Commerce

Le projet de loi sous avis (ci-après le « Projet ») a pour objet d'instituer les mesures d'application nationale 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 sur la cybersécurité (ci-après le « règlement (UE) n°2019/881 »).

En bref

- La Chambre de Commerce estime qu'il serait utile d'apporter des clarifications et adaptations à certaines dispositions du Projet, notamment en ce qui concerne les sanctions et l'autorité nationale de certification de cybersécurité.
- Elle s'interroge par ailleurs quant au degré suffisant d'indépendance fonctionnelle de la nouvelle autorité nationale.
- La Chambre de Commerce peut approuver le Projet, sous réserve de la prise en considération de ses commentaires.

Considérations générales

Le Projet vise à mettre en œuvre le règlement (UE) n°2019/881 en légiférant au niveau luxembourgeois sur les questions nécessitant une intervention législative nationale, telle que la désignation de l'autorité luxembourgeoise responsable pour la certification de cybersécurité. Son

[1] Lien vers le projet de loi sur le site de la Chambre des Députés

objectif est, comme indiqué par les auteurs du Projet dans l'exposé des motifs, d'exploiter les marges de manœuvre laissées au législateur national pour compléter et préciser certaines dispositions du règlement (UE) n°2019/881 telles que le rôle et les pouvoirs de l'autorité nationale de certification de cybersécurité.

Le règlement (UE) n°2019/881 réforme l'organisation de l'ENISA et vise à harmoniser la certification de cybersécurité (règles, exigences techniques, normes et procédures) au sein du marché intérieur. Il poursuit, *in fine*, les objectifs d'assurer au sein de l'Union européenne un niveau adéquat de sécurité informatique et d'éviter la fragmentation des schémas de certification, cette dernière situation étant souvent propice au protectionnisme entre les différents Etats membres. De plus, une certaine harmonisation de la certification de cybersécurité au niveau européen permettrait d'assurer une meilleure cybersécurité que des différents systèmes nationaux établis par chaque Etat membre isolément.

Conformément à l'exigence prévue à l'article 58 du règlement (UE) n°2019/881, le Projet désigne l'Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services (ci-après l'« ILNAS ») comme « *autorité nationale de certification de cybersécurité responsable des tâches de supervision* » et représentant du Luxembourg au sein du groupe européen de certification de cybersécurité. Il lui confie ainsi la charge des activités de supervision des organismes d'évaluation de la conformité, des émetteurs de déclarations de conformité de l'Union européenne et des titulaires de certificats de cybersécurité européens visés par le règlement (UE) n°2019/881.

Parallèlement, le Projet modifie la loi modifiée du 4 juillet 2014 portant réorganisation de l'ILNAS afin de confier à l'Organisme luxembourgeois de la confiance numérique nouvellement créé et remplaçant l'actuel département de la confiance numérique auprès de l'ILNAS, la mission d'assumer les tâches d'autorité nationale de certification de cybersécurité. En effet, les dispositions de l'article 58 du règlement (UE) n°2019/881 prévoient que les activités des autorités nationales de certification de cybersécurité liées à la certification doivent être strictement distinctes des activités de supervision et exécutées indépendamment l'une de l'autre.

Aussi, le Projet prévoit les sanctions administratives que l'ILNAS peut infliger respectivement aux émetteurs de déclarations de conformité de l'Union européenne, aux titulaires de certificats de cybersécurité européens et aux organismes d'évaluation de la conformité ainsi que les sanctions pénales.

Commentaire des articles

Concernant l'article 8 paragraphe 5

Dans le cadre d'un constat d'une « *violation grave par un titulaire de certificats, d'un émetteur d'une déclaration de conformité ou d'un organisme d'évaluation de la conformité des exigences fixées dans le règlement (UE) n°2019/881, des actes d'exécution pris en son exécution, des schémas européens de certification de cybersécurité, à la législation européenne applicable et à la présente loi* », le Projet prévoit que l'autorité nationale a la possibilité d'en informer les ministères compétents. La Chambre de Commerce suggère de substituer cette possibilité par une obligation puisque l'échange d'informations constitue une pratique essentielle dans le cadre de la cybersécurité.

Concernant l'article 8 paragraphe 6

Le Projet prévoit que l'autorité nationale de certification de cybersécurité peut faire appel à des experts externes pour procéder à « *des vérifications dans le contexte de l'octroi du maintien ou*

du retrait d'un certificat de cybersécurité européen ou d'une publication d'une déclaration de conformité de l'Union européenne ». Dans ce cadre, une couverture de « *frais d'experts* » est mentionnée sans plus de détails, ce que la Chambre de Commerce regrette. Des informations complémentaires, sur ce qui est couvert et ce qui ne l'est pas, permettraient en effet davantage de sécurité juridique.

Concernant les articles 9 et 10

Les articles 9 et 10 du Projet traitent des sanctions administratives et pénales que l'ILNAS peut infliger en cas de manquements aux dispositions du règlement (UE) n°2019/881 et des schémas européens de certification de cybersécurité.

Force est de constater que certaines dispositions (l'article 9 paragraphe 4 lettres g) et h) et l'article 10 paragraphe 1er lettres b) et c)) prévoient des sanctions administratives et des sanctions pénales à l'encontre des titulaires de certificats de cybersécurité européens pour les mêmes faits. La Chambre de Commerce estime qu'il conviendra d'apprécier si l'application par l'ILNAS d'une sanction administrative et l'application par une autorité judiciaire d'une sanction pénale ne pourrait conduire, dans des cas concrets, à sanctionner un titulaire de certificats de cybersécurité européens deux fois pour les mêmes faits et se ainsi éventuellement heurter au principe *non bis in idem*.

Concernant l'article 11

L'article 11 du Projet modifie la loi modifiée du 4 juillet 2014 portant réorganisation de l'ILNAS afin de confier à l'Organisme luxembourgeois de la confiance numérique nouvellement créé et remplaçant l'actuel département de la confiance numérique auprès de l'ILNAS la mission d'assumer les tâches d'autorité nationale de certification de cybersécurité. En effet, les dispositions de l'article 58 du règlement (UE) n°2019/881 prévoient que les activités des autorités nationales de certification de cybersécurité liées à la certification doivent être strictement distinctes des activités de supervision et exécutées indépendamment l'une de l'autre.

La Chambre de Commerce comprend que ledit Organisme luxembourgeois de la confiance numérique devrait assumer les tâches d'autorité nationale de certification de cybersécurité. Etant donné que l'Organisme luxembourgeois de la confiance numérique représente une subdivision de l'ILNAS, à qui le Projet confie le rôle de l'autorité nationale de certification de cybersécurité responsable des tâches de supervision, la Chambre de Commerce s'interroge quant à savoir si l'Organisme luxembourgeois de la confiance numérique dispose d'une indépendance opérationnelle effective suffisante afin d'exercer cette mission conformément aux dispositions de l'article 58 du règlement (UE) n°2019/881 exigeant une distinction stricte des missions de supervision et des missions de certification.

* * *

Après consultation de ses ressortissants, la Chambre de Commerce peut approuver le projet de loi sous avis, sous réserve de la prise en considération de ses commentaires.

NHO/GKA/DJI