N° 8132[6]

CHAMBRE DES DEPUTES

PROJET DE LOI

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 COMPLEMENTAIRE DE LA CHAMBRE DE COMMERCE

(17.7.2024)

Les amendements parlementaires au projet de loi n°8132 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, visent essentiellement à prendre en compte et à répondre aux observations et aux oppositions formelles formulées par le Conseil d'Etat dans son avis du 29 juin 2023.

En bref

- La Chambre de Commerce réitère son interrogation quant à savoir si l'Organisme luxembourgeois de la confiance numérique dispose d'une indépendance opérationnelle effective.
- Elle observe que les amendements parlementaires procèdent à la restructuration complète des dispositions relatives aux sanctions. Le projet de loi n°8132 prévoit désormais exclusivement des sanctions administratives, avec cependant semble-t-il, encore certains doublons qui seraient à supprimer.
- La Chambre de Commerce est en mesure d'approuver les amendements parlementaires sous avis, sous réserve de la prise en compte de ses commentaires.

*

CONSIDERATIONS GENERALES

La Chambre de Commerce avait déjà eu l'occasion de commenter, dans son avis du 1er août 2023 (ci-après l'« Avis Initial »), le projet de loi n°8132 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.

Pour rappel, le projet de loi n°8132 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 »).

Le projet de loi n°8132 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 confie 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. A noter que 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 s'est interrogée dans son Avis Initial 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 qui exigent une distinction stricte des missions de supervision et des missions de certification.

Les auteurs des amendements parlementaires sous avis précisent qu'ils ont eu l'assurance que l'ILNAS mettra en place des mesures visant à garantir cette indépendance et que ces mesures feront l'objet des examens par les pairs, tels que décrits dans l'article 59 du Règlement (UE) n°2019/881[1].

La Chambre de Commerce se demande toutefois si cet examen par les pairs permettra d'assurer une indépendance opérationnelle effective suffisante afin de répondre à l'exigence d'une distinction stricte des missions de supervision et des missions de certification.

Le projet de loi n°8132 prévoyait initialement **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**. La Chambre de Commerce a estimé dans son Avis Initial qu'il conviendrait d'apprécier si l'application par l'ILNAS d'une sanction administrative et l'application par une autorité

---

1 L'article 59 du Règlement (UE) n°2019/881 intitulé « Examen par les pairs » précise que :

« *1. Dans un souci d'équivalence des normes, dans l'ensemble de l'Union, en ce qui concerne les certificats de cyber sécurité européens et les déclarations de conformité de l'Union européenne, les autorités nationales de certification de cybersécurité font l'objet d'un examen par les pairs.*

2. L'examen par les pairs est effectué selon des critères et des procédures d'évaluation cohérents et transparents, en particulier en ce qui concerne les exigences structurelles et celles relatives aux ressources humaines et aux processus, ainsi que la confidentialité et les plaintes.

3. L'examen par les pairs évalue :

a) lorsqu'il y a lieu, la question de savoir si les activités des autorités nationales de certification de cybersécurité liées à la délivrance de certificats de cybersécurité européens visées à l'article 56, paragraphe 5, point a), et à l'article 56, paragraphe 6, sont strictement distinctes des activités de supervision visées à l'article 58, et celle de savoir si ces activités sont exercées indépendamment l'une de l'autre ;

b) les procédures permettant de superviser et de faire respecter les règles relatives au contrôle du respect par les produits TIC, services TIC et processus TIC des certificats de cybersécurité européens, conformément à l'article 58, paragraphe 7, point a) ;

c) les procédures permettant de contrôler et de faire respecter les obligations des fabricants et des fournisseurs de produits TIC, services TIC ou processus TIC, conformément à l'article 58, paragraphe 7, point b) ;

d) les procédures permettant de contrôler, d'autoriser et de superviser les activités des organismes d'évaluation de la conformité ;

e) lorsqu'il y a lieu, la question de savoir si le personnel des autorités ou organismes qui délivrent des certificats pour un niveau d'assurance dit « élevé », conformément à l'article 56, paragraphe 6, dispose des compétences nécessaires.

4. L'examen par les pairs est réalisé au moins une fois tous les cinq ans par au moins deux autorités nationales de certification de cybersécurité d'autres États membres et par la Commission. L'ENISA peut participer à l'examen par les pairs.

5. La Commission peut adopter des actes d'exécution établissant un plan pour l'examen par les pairs couvrant une période d'au moins cinq ans et définissant les critères concernant la composition de l'équipe chargée de l'examen par les pairs, la méthode utilisée pour mener cet examen, ainsi que le programme, la fréquence et les autres tâches y afférentes. Lors de l'adoption de ces actes d'exécution, la Commission tient dûment compte des observations formulées par le GECC. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 66, paragraphe 2.

6. Les résultats des examens par les pairs sont examinés par le GECC, qui établit des résumés pouvant être rendu publics et qui émet, au besoin, des lignes directrices ou des recommandations sur les actions à entreprendre ou les mesures à prendre par les entités concernées. ».

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 ainsi éventuellement se heurter au principe *non bis in idem*.

Les auteurs des amendements parlementaires ont procédé à la restructuration complète des articles du projet de loi n°8132 relatifs aux sanctions. L'article 8 du projet de loi n°8132 prévoit désormais un régime de sanctions administratives à l'encontre des émetteurs de déclarations de conformité de l'Union européenne. Les nouveaux articles 9 à 11 traitent des sanctions administratives à l'encontre de titulaires de certificats de cybersécurité en fonction du niveau d'assurance. Le nouvel article 12 prévoit quant à lui les sanctions administratives à l'encontre d'organismes d'évaluation de la conformité calibrées aussi en fonction du niveau d'assurance. Les sanctions pénales se trouvent supprimées. Ainsi, le projet de loi n°8132 prévoit désormais exclusivement des sanctions administratives.

La Chambre de Commerce observe toutefois que les dispositions de l'article 10, paragraphe 1er, points 10° et 11°, et de l'article 10, paragraphe 2, points 2° et 3° sanctionnent les mêmes faits, mais en prévoyant des sanctions différentes. Les auteurs des amendements parlementaires devraient dès lors procéder à la suppression d'une des sanctions prévues.

La Chambre de Commerce n'a pas d'autres observations à émettre.

*

Après consultation de ses ressortissants, la Chambre de Commerce est en mesure d'approuver les amendements parlementaires sous avis, sous réserve de la prise en compte de ses commentaires.

Impression: CTIE – Division Imprimés et Fournitures de bureau