

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 et portant modification de la loi modifiée du 4 juillet 2014 portant réorganisation de l'ILNAS

Deuxième avis complémentaire du Conseil d'État

(22 octobre 2024)

Par dépêche du 8 juillet 2024, le président de la Chambre des députés a soumis à l'avis du Conseil d'État trois amendements parlementaires au projet de loi sous rubrique, adoptés par la Commission de l'économie, des PME, de l'énergie, de l'espace et du tourisme, ci-après « Commission ».

Les amendements étaient accompagnés de remarques préliminaires, d'un commentaire pour chacun des amendements ainsi que d'un texte coordonné du projet de loi sous avis reprenant l'ensemble des modifications effectuées par la Commission et destinées à donner suite à l'avis complémentaire du Conseil d'État du 11 juin 2024¹.

Le deuxième avis complémentaire de la Chambre de commerce a été communiqué au Conseil d'État en date du 6 août 2024.

Considérations générales

Les amendements formels proposés par la Commission ont pour objet de répondre à un certain nombre d'observations de principe formulées par le Conseil d'État dans son avis complémentaire précité du 11 juin 2024.

À la lecture du texte coordonné du projet de loi joint aux amendements, le Conseil d'État a encore constaté que la Commission a repris, au niveau du futur point 6° de l'article 3, paragraphe 2, de la loi modifiée du 4 juillet 2014 portant réorganisation de l'ILNAS, la formulation proposée par le Conseil d'État dans son avis complémentaire précité du 11 juin 2024. Le Conseil d'État s'était en effet opposé formellement au libellé du point 6° proposé par la Commission au vu du fait que la configuration de la mission attribuée à la Commission nationale de certification de cybersécurité à travers la première série d'amendements soumis au Conseil d'État le 11 avril 2024 débouchait sur l'introduction d'éléments supplémentaires par rapport au règlement européen et risquait ainsi d'entraver l'applicabilité directe de ce dernier.

¹ [Avis complémentaire du Conseil d'État du 11 juin 2024 \(n° CE 61.290\)](#).

La reprise par la Commission du texte proposé par le Conseil d'État lui permet de lever son opposition formelle.

Examen des amendements

Amendement 1

Moyennant l'amendement sous examen, la Commission a revu la formulation de l'article 1^{er} du projet de loi afin d'y préciser le champ de la responsabilité de l'Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services, ci-après « ILNAS ». La Commission a ainsi précisé le renvoi fait par la disposition à l'article 56, paragraphe 6, 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, ci-après « règlement (UE) n° 2019/881 », en le limitant à la lettre a) de la disposition.

D'après la Commission, cette précision serait de nature à contribuer à la mise en place d'une indépendance opérationnelle effective entre les tâches de certification et les tâches de supervision de l'ILNAS et à répondre ainsi aux critiques du Conseil d'État concernant l'absence de cette indépendance opérationnelle entre les différentes tâches.

Le Conseil d'État estime cependant que la tentative de mettre une certaine distance opérationnelle entre les activités de supervision et de certification de l'ILNAS à travers l'exclusion de la lettre b) du paragraphe 6 de l'article 56 du règlement (UE) n° 2019/881 du champ de la disposition sous revue est vouée à l'échec. Les dispositions figurant sous les lettres a) et b) du paragraphe 6 de l'article 56 ne définissent en effet pas à proprement dire le champ des responsabilités des autorités nationales de certification, mais contiennent certaines précisions concernant l'exercice par les autorités en question de leurs compétences en la matière.

Le Conseil d'État note ensuite que l'article 56 du règlement (UE) n° 2019/881 vise les seuls schémas européens de certification de cybersécurité adoptés au titre de l'article 49 du règlement et qui exigent un niveau d'assurance dit « élevé ». Les certificats en question doivent en principe être délivrés par une autorité nationale de certification de cybersécurité, les certificats des autres niveaux étant délivrés par les organismes d'évaluation de la conformité tel que cela est prévu à l'article 56, paragraphe 4, du règlement (UE) n° 2019/881.

Cette compétence de principe de l'autorité nationale de certification pour les certificats du niveau d'assurance dit « élevé » est ensuite aménagée au niveau des lettres a) et b) de l'article 56, paragraphe 6, du règlement.

Le Conseil d'État comprend la disposition de l'article 56, paragraphe 6, lettre a), du règlement (UE) n° 2019/881 comme couvrant l'hypothèse où le certificat du niveau dit « élevé » sera bien délivré par un organisme d'évaluation de la conformité, mais devra être approuvé préalablement par

l'autorité nationale de certification de cybersécurité, la responsabilité de cette dernière restant dans ce cas pleinement engagée.

La lettre b) vise ensuite l'hypothèse où, en présence d'un schéma européen de certification de cybersécurité adopté au titre de l'article 49 du règlement et qui exige un niveau d'assurance dit « élevé », l'autorité nationale compétente a délégué préalablement la tâche consistant à délivrer les certificats de cybersécurité européens en question à un organisme d'évaluation de la conformité. Dans ce cas de figure précis, l'administration se dessaisit d'un pouvoir qui lui est accordé par la législation en vigueur et dont l'exercice est confié ensuite à une autre personne juridique, en l'occurrence un organisme d'évaluation de la conformité, cette façon de procéder s'accompagnant d'un transfert de la responsabilité pour les actes qui seront posés dans ce contexte, le délégataire devenant responsable en lieu et place du délégant. Pour que ce dispositif fasse du sens, la responsabilité initiale pour l'exercice du pouvoir doit cependant résider dans le chef de l'administration.

Le Conseil d'État constate qu'en tout état de cause le texte proposé ne pourra pas faire l'économie d'une désignation d'une autorité nationale de certification pour couvrir les certificats du niveau d'assurance dit « élevé ». Comme il n'est pas dans les intentions des auteurs du projet de loi de créer deux autorités, l'une chargée de la surveillance et l'autre de la certification, l'ILNAS devra assumer les deux fonctions. Dans cette perspective, ce sera précisément la possibilité offerte par l'article 56, paragraphe 6, lettre b), du règlement (UE) n° 2019/881 qui permettra à l'ILNAS de mettre une certaine distance opérationnelle entre ses activités de surveillance et l'exercice de sa compétence en matière de certification au niveau d'assurance dit « élevé », compétence qui se résumera à une compétence de principe qui pourra ensuite être déléguée aux organismes d'évaluation de la conformité.

Le Conseil d'État propose dès lors de se limiter en l'occurrence à désigner l'ILNAS comme « responsable des tâches de certification pour les certificats européens de cybersécurité du niveau d'assurance dit « élevé » visés à l'article 56 du règlement (UE) n° 2019/881 précité ».

Amendements 2 et 3

Les amendements 2 et 3 visent à reconfigurer le dispositif des sanctions qui peuvent être infligées conformément aux propositions formulées par le Conseil d'État dans son avis précité du 11 juin 2024.

Le Conseil d'État y marque son accord.

Ainsi délibéré en séance plénière et adopté à l'unanimité des 17 votants, le 22 octobre 2024.

Pour le Secrétaire général,
L'Attaché,

s. Ben Segalla

Le Président,

s. Marc Thewes