N° 8132[9]

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

* * *

RAPPORT DE LA COMMISSION DE L'ECONOMIE, DES PME, DE L'ENERGIE, DE L'ESPACE ET DU TOURISME

(5.12.2024)

La commission se compose de : Mme Carole HARTMANN, Président ; M. Guy ARENDT, Rapporteur ; Mme Diane ADEHM, M. André BAULER, M. Marc BAUM, M. Jeff BOONEN, M. Franz FAYOT, M. Patrick GOLDSCHMIDT, M. Claude HAAGEN, Mme Paulette LENERT, Mme Octavie MODERT, M. Laurent MOSAR, M. Tom WEIDIG, Mme Joëlle WELFRING, Mme Stéphanie WEYDERT, Membres.

*

1) ANTECEDENTS

Le projet de loi n° 8132 a été déposé le 3 janvier 2023 à la Chambre des Députés.

Au texte gouvernemental étaient joints un exposé des motifs, un commentaire des articles, les fiches financière et d'évaluation d'impact, un texte coordonné de la loi du 4 juillet 2014 portant réorganisation de l'ILNAS ainsi que le règlement (UE) n° 2019/881 à mettre en œuvre.

Le 29 juin 2023, le Conseil d'Etat a rendu son avis.

L'avis de la Chambre de Commerce date du 1er août 2023.

Le 14 mars 2024, la Commission de l'Economie, des PME, de l'Energie, de l'Espace et du Tourisme, ci-après la « commission », a examiné le texte du projet de loi ainsi que l'avis du Conseil d'Etat. Lors de cette même réunion, Monsieur Guy Arendt a été désigné comme rapporteur du projet de loi.

Le 11 avril 2024, la commission a adressé une lettre d'amendements pour avis complémentaire au Conseil d'Etat.

Le 11 juin 2024, le Conseil d'Etat a rendu son avis complémentaire.

Le 27 juin 2024, la commission a examiné l'avis complémentaire du Conseil d'Etat et a adressé, le 8 juillet 2024, une deuxième lettre d'amendements au Conseil d'Etat.

La Chambre de Commerce a publié son avis complémentaire le 17 juillet 2024 et son deuxième avis complémentaire le 29 juillet 2024.

Le 22 octobre 2024, le Conseil d'Etat a rendu son deuxième avis complémentaire, examiné par la commission lors de sa réunion du 21 novembre 2024.

Le 5 décembre 2024, la commission a adopté le présent rapport.

*

2) OBJET DU PROJET DE LOI

Le présent projet de loi vise la mise en place du règlement européen n° 2019/881 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, qui abroge le règlement (UE) n° 526/2013 (règlement sur la cybersécurité).

Ce règlement européen prévoit :

– un réaménagement du cadre organisationnel de l'ENISA ;
– une amélioration des conditions de fonctionnement du marché intérieur en consolidant le niveau de cybersécurité au sein de l'Union européenne par l'harmonisation des cadres de certification de cybersécurité européens. Ce dernier comprend des règles pour la certification, des normes, des exigences techniques qui permettent d'évaluer si les produits, les services ou les processus TIC (Technologies de l'information et de la communication) sont conformes.

Le projet de loi a également comme objectif de désigner l'autorité nationale de certification de cybersécurité et de compléter les dispositions du règlement, tout en respectant la marge de manœuvre accordée au législateur national. Il est question de définir les pouvoirs et le rôle du comité national de certification de cybersécurité et de l'autorité nationale de certification de cybersécurité, notamment de l'Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services – désigné ci-après par l'acronyme « ILNAS ».

Etant donné qu'au sein d'un même organisme les activités d'accréditation et de certification sont inconciliables et comme l'OLAS[1], au sein de l'ILNAS, représente l'organisme luxembourgeois d'accréditation et de surveillance, la fonction de l'ILNAS se limite strictement à la supervision et ne peut en aucun cas attribuer des certifications.

Les auteurs notent encore que le rôle de l'ENISA ainsi que la définition d'un cadre européen de certification de cybersécurité visent à :

– assurer un certain niveau de cybersécurité des produits, services et processus du type TIC sur le marché intérieur de l'Union européenne;
– empêcher la fragmentation du marché intérieur provoquée par la divergence des schémas de certification de cybersécurité, qui peuvent être considérés comme mesures de protectionnisme au sein de l'Union européenne.

Pour tout détail complémentaire, il est renvoyé au commentaire des articles.

*

3) AVIS

3.1) Avis de la Chambre de Commerce

Plutôt que de prévoir que l'autorité nationale a la possibilité d'informer les ministères compétents 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 » correspondant, 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.

La Chambre de Commerce regrette que la couverture de « frais d'experts » mentionnée dans le texte, dans le cadre d'un possible appel par l'autorité nationale de certification de cybersécurité à des experts externes, ne soit pas plus détaillée. Des informations supplémentaires fourniraient davantage de sécurité juridique. Le texte initial avait prévu des sanctions pénales et administratives et la Chambre de Commerce avait, dans ce contexte, soulevé le risque que le texte puisse se heurter au principe du *non bis in idem*. Avec la restructuration des dispositions afférentes, la Chambre s'interroge quant au maintien d'une partie seulement des sanctions pénales prévues au début.

---

1 Acronyme pour l'Office luxembourgeois d'accréditation et de surveillance

La Chambre de Commerce s'interroge si l'Organisme luxembourgeois de la confiance numérique dispose d'une indépendance opérationnelle effective suffisante afin d'exercer la mission lui confiée en matière de sa tâche d'autorité nationale de certification de cybersécurité. Bien que les auteurs aient clarifié le texte à cet égard par des amendements, la Chambre se demande dans son avis complémentaire si l' « 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 ». Malgré des amendements additionnels, la Chambre s'interroge dans son deuxième avis complémentaire si l'indépendance opérationnelle effective suffisante entre l'ILNAS comme « autorité nationale de certification de cybersécurité responsable des tâches de supervision » et l'Organisme luxembourgeois de la confiance numérique comme « autorité nationale de certification de cybersécurité » ne devrait pas se traduire par la mise à disposition d'un personnel propre, par des lignes hiérarchiques séparées et par des processus décisionnels distincts.

3.2) Avis du Conseil d'Etat

Dans son avis, la Haute Corporation remarque que les auteurs ont décidé de mettre en œuvre le règlement européen par un texte de loi autonome, comprenant des modifications apportées aux missions de l'ILNAS. En même temps, les auteurs ont revu la loi modifiée du 4 juillet 2014 en modifiant l'organisation de l'ILNAS afin que celle-ci soit en ligne avec ses nouvelles missions.

Cependant, le Conseil d'Etat aurait préféré que les missions de l'ILNAS soient définies dans un seul texte, en l'occurrence dans le texte de la loi du 4 juillet 2014.

La Haute Corporation a émis plusieurs oppositions formelles qui seront développées dans le cadre du commentaire des articles.

A la suite des amendements parlementaires, le Conseil d'Etat signale dans son avis complémentaire être en mesure de lever toutes les oppositions formelles, exceptée celle qui a été émise au niveau de l'article 3. En effet, la Haute Corporation juge que l'introduction de critères supplémentaires par rapport au règlement européen limiterait l'application directe de celui-ci. Dans cet ordre d'idées, le Conseil d'Etat a formulé une proposition de texte pour l'article 3. Ce libellé a été adopté par la commission.

Dans son deuxième avis complémentaire, le Conseil d'Etat note que la reprise du libellé proposé lui permet de lever ladite opposition formelle.

Pour le détail des observations du Conseil d'Etat et les décisions prises par la commission, il est renvoyé au commentaire ci-après.

*

4) COMMENTAIRE DES ARTICLES

Les adaptations d'ordre purement légistique effectuées dans la suite des avis du Conseil d'Etat ne seront pas commentées.

Chapitre 1er – Autorités compétentes et représentation nationale

Article 1er

L'article 1er désigne l'ILNAS comme Autorité nationale de certification de cybersécurité et de supervision au sens des articles 56 et 58 du règlement (UE) n° 2019/881 précité à mettre en œuvre.

La commission a précisé le libellé de cet article dans le sens des observations d'ordre légistique exprimées dans l'avis du Conseil d'Etat.

La commission a, par ailleurs, abandonné le raccourci projeté de « autorité nationale » pour désigner l'Autorité nationale de certification de cybersécurité. Dans l'ensemble du dispositif, il sera donc recouru au nom intégral de ladite autorité.

Quant à la préoccupation du Conseil d'Etat en ce qui concerne l'organisation de la nécessaire indépendance entre les activités de surveillance et de certification, telle qu'exigée à l'article 58, paragraphe 3, du règlement (UE) n° 2019/881, la commission a 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 même règlement (UE).

Dans son avis complémentaire, le libellé amendé de l'article 1er ne suscite pas d'observation de la part du Conseil d'Etat. Celui-ci maintient toutefois sa préoccupation évoquée et persiste à insister sur une indépendance opérationnelle effective des tâches de certification et celles de supervision.

En réaction, la commission a jugé utile de renvoyer de manière plus ciblée aux tâches de certification prévues et donc à la lettre a) du paragraphe 6 dudit article qui prévoit la délégation de cette tâche à un organisme d'évaluation de la conformité « moyennant l'approbation préalable de l'autorité nationale de certification de cybersécurité ».

Cette limitation à ladite lettre impliquait l'exclusion de la lettre b) de ce même paragraphe et visait donc à garantir l'indépendance opérationnelle effective de ces tâches.

En effet, pour les certificats du niveau d'assurance dit « élevé », l'ILNAS autorise au préalable un organisme d'évaluation de la conformité à procéder à un audit de certification. L'ILNAS n'effectue pas des audits de certification, mais autorise uniquement ces audits pour le niveau d'assurance dit « élevé ».

Les certificats des niveaux d'assurance dits « élémentaire » et « substantiel » sont délivrés par les organismes d'évaluation de la conformité, tel que prévu par l'article 56, paragraphe 4, du règlement (UE) n° 2019/881 précité.

Dans son deuxième avis complémentaire, le Conseil d'Etat « 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. » et explique pourquoi. En conclusion, le Conseil d'Etat souligne « 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. ».

Partant, le Conseil d'Etat propose « 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 ». ».

La commission a fait sienne cette proposition de reformulation de la fin du libellé de l'article 1er.

Article 2

L'article 2 précise que l'ILNAS est membre du groupe européen de certification de cybersécurité.

Article sans observation de la part du Conseil d'Etat.

Article 3

L'article 3 instaure un Comité national de certification de cybersécurité.

Le paragraphe 2 du présent article arrête les missions du Comité national de certification de cybersécurité.

Tandis que la modification apportée par la commission au premier point de l'énumération s'ensuit d'une observation légistique du Conseil d'Etat, la précision des parties prenantes évoquées au niveau de la lettre e)[2] vise à faire droit à l'observation afférente exprimée dans l'avis du Conseil d'Etat.

Le principal amendement effectué par la commission réside dans l'ajout d'un point supplémentaire. Cet ajout s'ensuit du choix du Gouvernement d'introduire également une certification au niveau d'assurance dit « élevé ».

Cet amendement suscite une série d'observations dans l'avis complémentaire du Conseil d'Etat qui s'oppose formellement au libellé proposé au motif que « la démarche proposée qui débouche clairement sur l'introduction de critères supplémentaires par rapport au règlement européen risque d'entraver l'applicabilité directe de ce dernier. »

---

2 Le mode d'énumération a également été adapté afin de le conformer aux règles légistiques.

Le Conseil d'Etat exprime toutefois une proposition de reformulation du point 6° qui permettrait de lever son opposition formelle. La commission a fait sienne cette proposition de texte.

Dans son deuxième avis complémentaire, le Conseil d'Etat constate que la reprise de sa proposition de texte lui permet de lever son opposition formelle.

Chapitre 2 – Obligations

Article 4

L'article 4 exige des titulaires de certificats de cybersécurité européens et des émetteurs de déclarations de conformité de l'Union européenne qu'ils affichent clairement les prix ainsi que les conditions de vente pour leurs produits, services et processus TIC.

Article sans observation de la part du Conseil d'Etat.

Article 5

L'article 5 prévoit certaines obligations pour les titulaires de certificats de cybersécurité européens, les émetteurs de déclaration de conformité de l'Union européenne et les organismes d'évaluation de la conformité dans leurs relations avec l'Autorité nationale de certification de cybersécurité.

Dans son avis, le Conseil d'Etat exprime une opposition formelle à l'encontre du premier paragraphe de l'article 5. Ce paragraphe oblige les entités relevant de l'Autorité nationale de certification de cybersécurité à lui accorder accès à tout ce dont elle a besoin pour assurer ses tâches. Le Conseil d'Etat se heurte à l'encadrement procédural insuffisant de ce pouvoir d'accès. Il rappelle, en outre, que ce pouvoir est soumis au respect du principe de proportionnalité, précise toutefois qu'il ne sera pas nécessaire de le viser expressément dans le corps de la loi « dans la mesure où le principe en question est reconnu comme principe de droit à valeur constitutionnelle par la Cour constitutionnelle. ».

Le Conseil d'Etat suggère « une solution qui renverrait expressément aux pouvoirs conférés à l'autorité nationale par le règlement européen, ce renvoi pouvant ensuite être complété, si nécessaire, par une énumération précise des pouvoirs supplémentaires dont le législateur national veut doter l'autorité pour exercer ses pouvoirs de supervision des acteurs du secteur. ».

Confronté à la proposition de la commission de renvoyer directement à l'article 58, paragraphe 8, lettre a), 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, le Conseil d'Etat rappelle dans son avis complémentaire « qu'il avait simplement exprimé une préférence pour une configuration, à un niveau général, du dispositif qui renverrait expressément aux pouvoirs conférés à l'autorité nationale par le règlement européen, ce renvoi pouvant ensuite être complété, si nécessaire, par une énumération précise des pouvoirs supplémentaires dont le législateur national voulait doter l'autorité pour exercer ses pouvoirs de supervision des acteurs du secteur. L'observation en question n'avait en tout cas aucun lien avec l'opposition formelle qui allait suivre. ».

Le Conseil d'Etat considère donc le renvoi introduit par amendement parlementaire comme superflu et comme pouvant être supprimé. La commission a fait sienne cette proposition et a retiré ce bout de phrase ajouté au paragraphe 1er.

La commission a également, et tout au long du dispositif, tel que proposé par le Conseil d'Etat, omis le qualificatif « européens » qu'elle avait ajouté à la désignation « organismes d'évaluation de la conformité ».

Constatant que le projet de loi sanctionne également pénalement le fait d'entraver les enquêtes de l'autorité nationale, le Conseil d'Etat souligne dans son avis initial qu'il « conviendrait de compléter ces sanctions par un dispositif procédural qui pourrait s'inspirer des dispositions de l'article 15, paragraphe 1er, alinéa 1er, de la loi précitée du 4 juillet 2014, qui fait intervenir les officiers et agents de police judiciaire de l'ILNAS lorsqu'il s'agit d'accéder aux locaux, installations, sites et moyens de transport à la condition que des indices graves faisant présumer une infraction existent. » Le Conseil d'Etat conclut en signalant que la reprise du dispositif évoqué pour compléter le présent article lui permettrait de lever son opposition formelle.

Par l'ajout d'un paragraphe supplémentaire (paragraphe 3 nouveau), qui reprend la disposition à laquelle le Conseil d'Etat renvoie, la commission a fait droit à l'avis du Conseil d'Etat.

Cependant, dans son avis complémentaire, le Conseil d'Etat attire l'attention de la commission au fait qu'elle a supprimé « l'ancien article 10 regroupant les sanctions pénales initialement prévues, de sorte que le projet de loi sous avis ne comporte plus que des sanctions administratives. Or, l'institution de l'officier de police judiciaire est propre à la procédure pénale et les prérogatives particulières que le Code de procédure pénale confère aux officiers de police judiciaire sont limitées à la recherche et à la constatation des infractions pénales. Par conséquent, l'intervention des officiers et agents de police judiciaire ne ferait plus de sens en l'occurrence. ».

Le Conseil d'Etat suggère également une issue à cette situation. Celle-ci consisterait à « réintroduire dans le projet de loi sous avis des dispositions qui sanctionnent pénalement le non-respect de l'article 58, paragraphe 8, lettre a), du règlement (UE) n° 2019/881 précité par un acteur du marché qui ne mettrait pas à la disposition de l'ILNAS toute information dont il a besoin pour l'exécution de ses tâches et de l'article 58, paragraphe 8, lettre b), du règlement (UE) n° 2019/881 précité par un acteur du marché qui entraverait les enquêtes de l'ILNAS. Parallèlement, les sanctions administratives prévues par le texte sous revue à l'endroit des organismes surveillés qui empêcheraient l'ILNAS d'exercer les pouvoirs qui lui sont conférés sur la base des dispositions précitées devront être retirées du texte afin d'éviter que les autorités concernées ne se trouvent en porte-à-faux par rapport à l'application du principe du *non bis in idem*. ». La commission a fait sienne cette suggestion et renvoie à ce sujet à son commentaire de l'article 13 nouveau.

Dans son avis complémentaire, le Conseil d'Etat note encore que le champ d'application du paragraphe 3 (nouveau) diffère de celui du paragraphe 1er qui vise « tout document, toute personne, tout équipement et tout local ». Partant, il propose de reformuler la fin de phrase du premier paragraphe du présent article afin de faire coïncider les champs des deux dispositions. La commission a fait droit à cette proposition.

Sans observation dans le deuxième avis complémentaire du Conseil d'Etat.

Article 6 (supprimé)

L'ancien article 6 rappelait le secret professionnel auquel les auditeurs sont tenus.

La commission a supprimé l'ancien article 6, pour donner suite à l'avis du Conseil d'Etat qui considère ce dispositif comme superfétatoire alors « que les cabinets d'audit sont déjà soumis à l'obligation du secret professionnel inscrite tant à l'article 458 du Code pénal qu'à l'article 28, paragraphe 1er, de la loi modifiée du 23 juillet 2016 relative à la profession de l'audit. ».

Sans observation de la part du Conseil d'Etat dans la suite.

Article 6 (ancien article 7)

L'article 6, renvoyant à l'article 60 du règlement (UE) n° 2019/881, regroupe les obligations des organismes d'évaluation de la conformité accrédités.

La commission a supprimé le premier paragraphe, considéré dans l'avis du Conseil d'Etat comme « à la limite » superfétatoire puisqu'il « ne fait que reproduire la substance de l'article 60 du règlement (UE) n° 2019/881 en imposant aux organismes d'évaluation de la conformité qui souhaitent certifier des produits TIC, des services TIC et des processus TIC l'obligation de se faire accréditer. »

Quoique sans observation de la part du Conseil d'Etat, la commission a également supprimé le paragraphe 3. Ce paragraphe se bornait à reprendre une disposition afférente du règlement (UE) n° 2019/881, règlement qui est d'application directe.

Sans observation dans les deux avis complémentaires du Conseil d'Etat.

Chapitre 3 – L'Autorité nationale de certification de cybersécurité

Article 7 (ancien article 8)

L'article 7 traite du rôle de l'Autorité nationale de certification de cybersécurité.

Cet article a été retravaillé de fond en comble non seulement en raison des observations exprimées directement à son égard dans l'avis du Conseil d'Etat, mais également en raison du réagencement, sur demande du Conseil d'Etat, du régime répressif prévu au chapitre 4. En effet, dans l'intérêt de la lisibilité, les sanctions ont été regroupées en fonction des entités visées.

Au paragraphe 1er, deuxième alinéa, et à la suite d'une question afférente soulevée par le Conseil d'Etat, la commission a corrigé l'accord du verbe « définir » – cette partie de phrase se rapportant à la notification dont a fait l'objet l'organisme d'évaluation de la conformité.

Au niveau de l'ancien paragraphe 2, la commission a repris la proposition de texte du Conseil d'Etat, tout en tenant compte de la restructuration du régime répressif prévu. Dans son avis, le Conseil d'Etat propose, en effet, une reformulation de ce paragraphe pour en faire ressortir plus clairement l'objectif, qui est d'accorder un délai afin que l'/les acteur(s) puisse(nt) se conformer aux exigences qui découlent des cas de figure précis repris à l'/aux article(s) 9 (et 10).

Les nouveaux paragraphes 2, 4 et 5 insérés respectent la logique rédactionnelle proposée par le Conseil d'Etat.

Tel que demandé par le Conseil d'Etat, l'ancien paragraphe 3 a été reformulé, afin d'exclure la lecture erronée à laquelle la première partie de la première phrase du libellé initial induisait.

L'ancien paragraphe 4 a été supprimé.

L'ancien paragraphe 5, au sujet duquel tant le Conseil d'Etat que la Chambre de Commerce suggèrent qu'en cas de violation grave les ministères compétents devraient être obligatoirement informés, a été supprimé.

Concernant l'ancien paragraphe 6, la commission donne à considérer que les audits de conformité (frais d'experts) sont toujours à charge des entités auditées. Tel que suggéré par le Conseil d'Etat, la précision que les vérifications, auxquelles l'Autorité nationale de certification de cybersécurité peut procéder, peuvent avoir lieu « , aussi sur demande dûment justifiée de personnes intéressées, » a été supprimée comme étant superfétatoire.

En réaction à la recommandation du Conseil d'Etat, « de détailler les frais d'experts qui seront « couverts » (…) » par les personnes contrôlées, la commission a ajouté une disposition supplémentaire.

Tel que proposé par le Conseil d'Etat, la deuxième phrase de l'ancien paragraphe 7 a été omise.

Dans son avis complémentaire, le Conseil d'Etat marque son accord avec la restructuration du dispositif et avec les reformulations effectuées.

Au niveau du détail, le Conseil d'Etat propose toutefois deux reformulations que la commission a fait siennes. Ainsi, le début du paragraphe 2 (nouveau) a été reformulé afin de mieux faire ressortir « que sont visées les déclarations faites par un fabricant ou un fournisseur de produits TIC, de services TIC ou de processus TIC qui, à la suite d'une autoévaluation de la conformité, délivre une déclaration de conformité de l'Union européenne indiquant que le respect des exigences énoncées dans le schéma européen de certification de cybersécurité pertinent a été démontré. Ce dispositif est limité aux produits, services et processus qui ne présentent qu'un risque faible correspondant au niveau d'assurance dit « élémentaire ». L'autre reformulation visait une référence faite par le paragraphe 6 (ancien paragraphe 3).

Concernant le paragraphe 8 ajouté par la commission en réaction à la recommandation du Conseil d'Etat, « de détailler les frais d'experts qui seront « couverts » (…) » par les personnes contrôlées, le Conseil Etat note que ce « texte est calqué sur celui de l'article 4, paragraphe 2, de la loi précitée du 4 juillet 2014, qui reprend l'ensemble des frais qui sont refacturés aux entités supervisées. » et « peut marquer son accord avec cette façon de procéder. ».

Sans observation dans le deuxième avis complémentaire du Conseil d'Etat.

Chapitre 4 – Sanctions

Article 8 (ancien article 9)

Initialement, cet article définissait le régime de sanctions administratives prévues pour l'ensemble des acteurs en matière de cybersécurité.

Désormais, l'article 8 regroupe les seules sanctions administratives que l'ILNAS peut appliquer à l'encontre des émetteurs de déclarations de conformité de l'Union européenne, en cas de manquement aux dispositions du règlement (UE) n° 2019/881 et des schémas européens de certification de cybersécurité.

Dans son avis, le Conseil d'Etat s'oppose formellement au double régime répressif prévu, administratif et pénal (anciens articles 9 et 10).

Le Conseil d'Etat constate que le dispositif prévoit « des sanctions administratives et des sanctions pénales pour les mêmes acteurs, à savoir les titulaires de certificats de cybersécurité européens, au niveau d'assurance dit substantiel, pour (…) des infractions à l'article 58, paragraphe 8, point a°, du règlement (UE) n° 2019/881 (non mise à la disposition de l'ILNAS de toute information dont l'administration a besoin pour l'exécution de ses tâches), et à l'article 58, paragraphe 8, point b°, du règlement (UE) n° 2019/881 (entrave aux enquêtes de l'ILNAS) ». Partant, le Conseil d'Etat souligne que cette « approche comporte le risque que dans une même affaire, l'ILNAS puisse infliger une amende administrative et les autorités judiciaires une amende pénale pour sanctionner les mêmes faits, façon de procéder qui se heurterait au principe *non bis in idem* (…) et exige que les auteurs optent en l'occurrence pour une des deux voies de répression, administrative ou pénale. ».

Dans une première réaction, la commission a limité le régime répressif du dispositif à des sanctions administratives. Elle a, en outre, subdivisé ce régime en fonction des niveaux d'assurance.

Pour les titulaires de certificats de cybersécurité, trois articles distincts sont désormais prévus, un article pour chaque niveau d'assurance (articles 9, 10 et 11 nouveaux).

Pour les titulaires de certificats de cybersécurité aux niveaux d'assurance dits « substantiel » (article 10 nouveau) et « élevé » (article 11 nouveau) deux niveaux de sanctions ont été définis. La sévérité de la sanction dépend de l'impact potentiel de l'infraction sur les clients du titulaire du certificat de cybersécurité respectif.

Les dispositions visant les organismes d'évaluation de la conformité (paragraphe 5 de l'ancien article 9) ont été restructurées afin de refléter l'impact potentiel des infractions commises. Ces dispositions se retrouvent regroupées au niveau de l'article 12 (nouveau).

Dans le cadre de sa deuxième série d'amendements, la commission a supprimé, tel que suggéré dans l'avis complémentaire du Conseil d'Etat, les sanctions administratives prévues en cas de non-respect des lettres a) et b) du paragraphe 8 de l'article 58 du règlement (UE) n° 2019/881 précité, à savoir le fait de ne pas mettre à disposition de l'ILNAS toute information dont il a besoin pour l'exécution de ses tâches et le fait d'entraver ses enquêtes.

Dorénavant, ces infractions seront sanctionnées pénalement. A ce sujet, la commission renvoie à son commentaire de l'article 13 (nouveau).

Cette approche évince également le doublon signalé dans l'avis complémentaire du Conseil d'Etat au niveau de l'article 10 où les mêmes faits sont incriminés aux paragraphes 1er (points 10° et 11°) et 2 (points 2° et 3°).

Dans son deuxième avis complémentaire, le Conseil d'Etat marque son accord à ces ultimes amendements.

Article 9 (nouveau)

L'article 9 regroupe les sanctions administratives applicables à l'encontre de titulaires de certificats de cybersécurité au niveau d'assurance dit « élémentaire ».

Cet article a été introduit dans le contexte de la première série d'amendements parlementaires rédigés pour donner suite à l'avis du Conseil d'Etat. A ce sujet, la commission renvoie à son commentaire de l'article 8 (ancien article 9).

Article 10 (nouveau)

L'article 10 regroupe les sanctions administratives applicables à l'encontre de titulaires de certificats de cybersécurité au niveau d'assurance dit « substantiel ».

Cet article a été introduit dans le contexte de la première série d'amendements parlementaires rédigés pour donner suite à l'avis du Conseil d'Etat. A ce sujet, la commission renvoie à son commentaire de l'article 8 (ancien article 9).

Article 11 (nouveau)

L'article 11 regroupe les sanctions administratives applicables à l'encontre de titulaires de certificats de cybersécurité au niveau d'assurance dit « élevé ».

Cet article a été introduit dans le contexte de la première série d'amendements parlementaires rédigés pour donner suite à l'avis du Conseil d'Etat. A ce sujet, la commission renvoie à son commentaire de l'article 8 (ancien article 9).

Article 12 (nouveau)

L'article 12 regroupe les sanctions administratives applicables à l'encontre d'organismes d'évaluation de la conformité.

Cet article a été introduit dans le contexte de la première série d'amendements parlementaires rédigés pour donner suite à l'avis du Conseil d'Etat. A ce sujet, la commission renvoie à son commentaire de l'article 8 (ancien article 9).

Article 13 (ancien article 10)

L'article 13 prévoit des sanctions pénales.

Initialement, dans le contexte de l'amendement ayant visé l'ancien article 9 et afin de faire droit à une opposition formelle du Conseil d'Etat, la commission avait intégralement supprimé l'ancien article 10.

Cependant, tel que suggéré dans l'avis complémentaire du Conseil d'Etat, la commission a réintroduit deux infractions pénales – tout en supprimant les sanctions administratives prévues pour les deux dispositions visées, les lettres a) et b) du paragraphe 8 de l'article 58 du règlement (UE) n° 2019/881 précité, afin d'exclure une entorse au principe du *non bis in idem*.

Ce retour partiel au texte initial s'explique par la volonté de maintenir la possibilité de faire intervenir des officiers et agents de police judiciaire tel que prévu par l'article 5, paragraphe 3, du dispositif légal. La commission renvoie à son commentaire dudit article.

Dans son deuxième avis complémentaire, le Conseil d'Etat marque son accord à la reconfiguration projetée du dispositif des sanctions qui peuvent être infligées.

Chapitre 5 – Dispositions modificatives

Article 14 (ancien article 11)

L'article 14 prévoit deux modifications dans la loi modifiée du 4 juillet 2014 portant réorganisation de l'ILNAS : le « département de la confiance numérique » est renommé « Organisme luxembourgeois de la confiance numérique » et un point 6° est ajouté au niveau de l'article 4 de la même loi.

Dans son avis, le Conseil d'Etat renvoie à ses observations exprimées à l'endroit de l'article 1er du projet de loi.

La commission s'est limitée à faire droit aux observations d'ordre légistique du Conseil d'Etat visant cet article.

Sans observation dans les avis complémentaires du Conseil d'Etat.

*

5) TEXTE PROPOSE PAR LA COMMISSION

Compte tenu de ce qui précède, la Commission de l'Economie, des PME, de l'Energie, de l'Espace et du Tourisme recommande à la Chambre des Députés d'adopter le projet de loi n° 8132 dans la teneur qui suit :

*

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

Chapitre 1er – Autorités compétentes et représentation nationale

Art. 1er. Autorité nationale de certification de cybersécurité

L'Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services, ci-après « ILNAS », est désigné comme Autorité nationale de certification de cybersécurité responsable des tâches de supervision au sens de l'article 58 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), tel que modifié, et 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.

Art. 2. Groupe européen de certification de cybersécurité

L'ILNAS, en tant qu'Autorité nationale de certification de cybersécurité, participe au Groupe européen de certification de cybersécurité au sens de l'article 62 du règlement (UE) n° 2019/881 précité.

Art. 3. Comité national de certification de cybersécurité

(1) Un Comité national de certification de cybersécurité, ci-après « comité », est créé auprès du ministre ayant l'Economie dans ses attributions, dont la composition et l'organisation sont déterminées par règlement grand-ducal.

(2) Le comité a les missions suivantes :

1° conseiller le ministre en ce qui concerne le programme de travail glissant de l'Union européenne pour la certification européenne de cybersécurité ;

2° prendre position sur la politique de certification de cybersécurité de l'Union européenne ;

3° prendre position sur les schémas européens de certification de cybersécurité ;

4° prendre position sur la maintenance et le réexamen des schémas européens de certification de cybersécurité existants ;

5° informer les parties prenantes concernées, les entreprises du secteur des TIC, les fournisseurs de réseaux ou de services de communications électroniques accessibles au public, les PME, les opérateurs de services essentiels, les organisations de consommateurs, les experts universitaires en matière de cybersécurité ainsi que les autorités chargées de l'application de la loi et les autorités de contrôle de la protection des données du processus consultatif prévu à l'article 56, paragraphe 3, alinéa 3, lettre c), du règlement (UE) n° 2019/881 précité ;

6° conseiller le ministre, par schéma de certification, en ce qui concerne l'application des objectifs et éléments définis par le règlement (UE) n° 2019/881 précité qui sont pris en compte pour délivrer, en application de l'article 56, paragraphe 6, lettre a), dudit règlement (UE) n° 2019/881, un certificat de cybersécurité au niveau d'assurance dit « élevé ».

Chapitre 2 – Obligations

Section 1re – Obligations générales d'information

Art. 4. Accès aux informations

Lorsque les produits, services et processus des technologies de l'information et de la communication (TIC) des titulaires de certificats de cybersécurité européens et des émetteurs de déclarations de conformité de l'Union européenne font mention de prix et conditions de vente ou de réalisation de la prestation, ces derniers doivent être indiqués de manière précise et non équivoque. Il doit aussi être indiqué si toutes les taxes et frais additionnels sont compris dans le prix.

Art. 5. Echanges avec l'Autorité nationale de certification de cybersécurité

(1) Les titulaires de certificats de cybersécurité européens, les émetteurs de déclarations de conformité de l'Union européenne et les organismes d'évaluation de la conformité donnent accès à l'Autorité nationale de certification de cybersécurité à tout document, toute personne, tout équipement, tout local, toute installation, tout site et tout moyen de transport dont elle a besoin pour pouvoir assurer ses tâches.

(2) Les titulaires de certificats de cybersécurité européens, les émetteurs de déclarations de conformité de l'Union européenne et les organismes d'évaluation de la conformité informent l'Autorité nationale de certification de cybersécurité par écrit dans un délai de soixante-douze heures après avoir eu connaissance d'une vulnérabilité ou irrégularité qui est susceptible d'avoir une incidence sur le respect des exigences de sécurité liées à la certification d'un produit, d'un service ou d'un processus selon le règlement (UE) n° 2019/881 précité.

(3) Les officiers et agents de police judiciaire visés à l'article 10 du Code de procédure pénale et les personnes visées à l'article 14, paragraphe 1er, de la loi modifiée du 4 juillet 2014 portant réorganisation de l'ILNAS ont accès aux locaux, installations, sites et moyens de transport assujettis à la présente loi et aux règlements pris en son exécution. Ils peuvent pénétrer de jour et de nuit, lorsqu'il existe des indices graves faisant présumer une infraction à la présente loi et à ses règlements d'exécution, dans les locaux, installations, sites et moyens de transport visés ci-dessus. Ils signalent leur présence au chef du local, de l'installation ou du site ou à celui qui le remplace. Celui-ci a le droit de les accompagner lors de la visite.

Section 2 – Les organismes d'évaluation de la conformité

Art. 6. Obligations des organismes d'évaluation de la conformité

(1) L'organisme d'évaluation de la conformité accrédité au sens de l'article 60 du règlement (UE) n° 2019/881 précité informe, dans un délai de soixante-douze heures, l'Autorité nationale de certification de cybersécurité de son accréditation.

(2) L'Autorité nationale de certification de cybersécurité doit toujours être tenue informée, dans un délai de soixante-douze heures, des certificats délivrés par l'organisme d'évaluation de la conformité dans le cadre de l'article 60 du règlement (UE) n° 2019/881 précité.

Chapitre 3 – L'Autorité nationale de certification de cybersécurité

Art. 7. Rôle de l'Autorité nationale de certification de cybersécurité

(1) L'Autorité nationale de certification de cybersécurité notifie tout organisme d'évaluation de la conformité accrédité à la Commission européenne, conformément à l'article 61 du règlement (UE) n° 2019/881 précité, et le cas échéant, autorisé au sens de l'article 58, paragraphe 7, lettre e), qui certifie des produits TIC, des services TIC et processus TIC, dans le cadre d'un schéma européen de certification de cybersécurité aux niveaux d'assurances déterminés en vertu de l'article 52 du règlement (UE) n° 2019/881 précité.

L'Autorité nationale de certification de cybersécurité peut présenter à la Commission européenne une demande visant à retirer de la liste des organismes d'évaluation de la conformité, les organismes d'évaluation de la conformité qui ont fait l'objet d'une notification dans le cadre d'un schéma européen

de certification de cybersécurité, tel que définie dans l'article 61 du règlement (UE) n° 2019/881 précité sur demande de l'organisme d'évaluation de la conformité ou si l'organisme d'évaluation de la conformité n'est pas conforme aux exigences du règlement (UE) n° 2019/881 précité, des actes d'exécution pris en son exécution, des schémas européens de certification de cybersécurité correspondants et à la présente loi.

(2) Si l'Autorité nationale de certification de cybersécurité constate qu'un émetteur de déclarations de conformité de l'Union Européenne, telles que visées à l'article 53 du règlement (UE) n° 2019/881 précité, a un comportement visé à l'article 8 et sanctionné par ce même article, elle invite l'émetteur de déclarations de conformité de l'Union Européenne à y remédier, dans les délais qu'elle détermine. Si passé ce délai, l'émetteur de déclarations de conformité de l'Union Européenne n'y a pas remédié, l'autorité nationale de certification de cybersécurité peut appliquer les sanctions administratives afférentes prévues à l'article 8.

(3) Si l'Autorité nationale de certification de cybersécurité constate qu'un titulaire de certificat de cybersécurité au niveau d'assurance dit « élémentaire », tel que défini à l'article 52 du règlement (UE) n° 2019/881 précité, a un comportement visé à l'article 9 et sanctionné par ce même article, elle invite le titulaire de certificat de cybersécurité à y remédier, dans les délais qu'elle détermine. Passé ce délai, l'Autorité nationale de certification de cybersécurité peut appliquer les sanctions administratives afférentes prévues à l'article 9.

(4) Si l'Autorité nationale de certification de cybersécurité constate qu'un titulaire de certificat de cybersécurité au niveau d'assurance dit « substantiel », tel que défini à l'article 52 du règlement (UE) n° 2019/881 précité, a un comportement visé à l'article 10 et sanctionné par ce même article, elle invite le titulaire de certificat de cybersécurité à y remédier, dans les délais qu'elle détermine. Si, passé ce délai, le titulaire de certificat n'y a pas remédié, l'Autorité nationale de certification de cybersécurité peut appliquer les sanctions administratives afférentes prévues à l'article 10.

(5) Si l'Autorité nationale de certification de cybersécurité constate qu'un titulaire de certificat de cybersécurité au niveau d'assurance dit « élevé », tel que défini à l'article 52 du règlement (UE) n° 2019/881 précité, a un comportement visé à l'article 11 et sanctionné par ce même article, elle invite le titulaire de certificat de cybersécurité à y remédier, dans les délais qu'elle détermine. Si, passé ce délai, le titulaire de certificat n'y a pas remédié, l'Autorité nationale de certification de cybersécurité peut appliquer les sanctions administratives afférentes prévues à l'article 11.

(6) Si l'Autorité nationale de certification de cybersécurité constate qu'un organisme d'évaluation de la conformité qui émet des certificats de cybersécurité européens aux niveaux d'assurance tels que définis à l'article 52 du règlement (UE) n° 2019/881 précité, a un comportement visé à l'article 12 et sanctionné par ce même article, elle invite l'organisme d'évaluation de la conformité à y remédier, dans les délais qu'elle détermine. Si, passé ce délai, l'organisme d'évaluation de la conformité n'y a pas remédié, l'Autorité nationale de certification de cybersécurité peut appliquer les sanctions administratives afférentes prévues à l'article 12.

(7) L'Autorité nationale de certification de cybersécurité peut procéder à tout moment 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. L'Autorité nationale de certification de cybersécurité peut avoir recours à des experts externes pour effectuer ces vérifications. Les frais d'experts sont refacturés aux titulaires de certificats de cybersécurité européens, aux émetteurs de déclarations de conformité de l'Union européenne et aux organismes d'évaluation de la conformité.

(8) Les frais relatifs à la préparation des contrôles, les frais des contrôles proprement dits, ainsi que les frais relatifs à la rédaction des rapports de contrôle, sont refacturés aux entités supervisées prévues à l'article 58, paragraphe 7, du règlement (UE) n° 2019/881 précité. Le barème tarifaire, approuvé par le ministre, est publié sur le site électronique installé à cet effet par l'ILNAS.

(9) L'Autorité nationale de certification de cybersécurité peut collaborer avec d'autres autorités compétentes dans un autre Etat membre pour exécuter ses tâches de supervision.

(10) L'Autorité nationale de certification de cybersécurité peut, dès lors que c'est dans l'intérêt public, publier soit au Journal officiel du Grand-Duché de Luxembourg, soit dans un ou plusieurs journaux luxembourgeois ou étrangers, un retrait d'un certificat de cybersécurité européen.

Chapitre 4 – Sanctions

Art. 8. Sanctions administratives à l'encontre d'émetteurs de déclarations de conformité de l'Union européenne

(1) Le directeur de l'ILNAS peut infliger une amende administrative de 250 euros à 25 000 euros aux émetteurs de déclarations de conformité de l'Union européenne qui enfreignent :

1° l'article 53, paragraphe 1er, du règlement (UE) n° 2019/881 précité, en produisant des déclarations de conformité d'un niveau autre que « élémentaire » ;

2° l'article 54, paragraphe 1er, lettre e), du règlement (UE) n° 2019/881 précité, en publiant des déclarations de conformité alors que ce n'est pas prévu dans le schéma européen de certification ;

3° les dispositions du schéma européen de certification de cybersécurité concernant l'utilisation des labels et des marques conformément à l'article 54, paragraphe 1er, lettre i), du règlement (UE) n° 2019/881 précité ;

4° l'article 53, paragraphe 2, du règlement (UE) n° 2019/881 précité et les dispositions du schéma européen de certification de cybersécurité concernant les contrôles préalables à la publication des déclarations de conformité des exigences relatives à l'article 54, paragraphe 1er, lettre j), du règlement (UE) n° 2019/881 précité ;

5° les dispositions du schéma européen de certification de cybersécurité concernant les conséquences résultant du contrôle des exigences et ne mettent pas à jour les déclarations de conformité conformément à l'article 54, paragraphe 1er, lettre l), du règlement (UE) n° 2019/881 précité ;

6° les dispositions du schéma européen de certification de cybersécurité concernant le traitement des vulnérabilités de cybersécurité non détectées précédemment conformément aux articles 54, paragraphe 1er, lettre m), et 56, paragraphe 8, du règlement (UE) n° 2019/881 précité ;

7° les dispositions du schéma européen de certification de cybersécurité concernant le format ou le contenu des déclarations de conformité conformément à l'article 54, paragraphe 1er, lettre p), du règlement (UE) n° 2019/881 précité ;

8° l'article 53, paragraphe 3 du règlement (UE) n° 2019/881 précité et les dispositions du schéma européen de certification de cybersécurité de l'article 54, paragraphe 1er, lettre q), du règlement (UE) n° 2019/881 précité, concernant la disponibilité de la déclaration de conformité ;

9° l'article 55 du règlement (UE) n° 2019/881 précité, en ne mettant les informations supplémentaires spécifiées dans le schéma européen de certification de cybersécurité pas à disposition du public ou en ne les mettant pas à jour.

(2) L'Administration de l'enregistrement, des domaines et de la TVA est chargée du recouvrement des amendes qui lui sont communiquées par le directeur de l'administration compétente. Le recouvrement est poursuivi comme en matière d'enregistrement.

(3) Les décisions d'infliger une amende administrative en vertu du présent article sont susceptibles d'un recours en réformation à introduire devant le tribunal administratif, dans le délai de trois mois à compter de la notification.

Art. 9. Sanctions administratives à l'encontre de titulaires de certificats de cybersécurité au niveau d'assurance dit « élémentaire »

(1) Le directeur de l'ILNAS peut infliger une amende administrative de 250 euros à 25 000 euros aux titulaires de certificats de cybersécurité européens au niveau d'assurance dit « élémentaire » qui enfreignent :

1° les articles 55, paragraphe 1er, lettres a), b), c) ou d), ou 55, paragraphe 2, du règlement (UE) n° 2019/881 précité, en ne mettant les informations supplémentaires spécifiées dans le schéma européen de certification de cybersécurité pas à disposition du public ou en ne les mettant pas à jour ;

2° les articles 52, paragraphe 2, et 54, paragraphe 1er, lettre d), du règlement (UE) n° 2019/881 précité, en publiant des informations par rapport à leur certification sans spécifier le niveau d'assurance ;

3° les dispositions du schéma européen de certification de cybersécurité concernant l'utilisation des labels et des marques conformément à l'article 54, paragraphe 1er, lettre i), du règlement (UE) n° 2019/881 précité ;

4° les dispositions du schéma européen de certification de cybersécurité concernant son champ d'application relatives à l'article 54, paragraphe 1er, lettre a), du règlement (UE) n° 2019/881 précité, en ne mettant pas ces informations à disposition du public ;

5° les dispositions du schéma européen de certification de cybersécurité concernant le traitement des vulnérabilités de cybersécurité non détectées précédemment conformément aux articles 54, paragraphe 1er, lettre m), et 56, paragraphe 8, du règlement (UE) n° 2019/881 précité ;

6° les dispositions du schéma européen de certification de cybersécurité concernant le format ou le contenu des certificats de cybersécurité européens conformément à l'article 54, paragraphe 1er, lettre p), du règlement (UE) n° 2019/881 précité ;

7° les dispositions du schéma européen de certification de cybersécurité concernant la période de disponibilité de la documentation technique ou de toutes les autres informations pertinentes qui sont mises à disposition par le fabricant ou le fournisseur de produits TIC, services TIC ou processus TIC, conformément aux articles 53, paragraphe 3, et 54, paragraphe 1er, lettre q), du règlement (UE) n° 2019/881 précité ;

8° les dispositions du schéma européen de certification de cybersécurité concernant la durée maximale de validité des certificats conformément à l'article 54, paragraphe 1er, lettre r), du règlement (UE) n° 2019/881 précité ;

9° l'article 56, paragraphe 7, du règlement (UE) n° 2019/881 précité, en ne mettant pas à disposition de l'ILNAS ou de l'organisme d'évaluation de la conformité les informations nécessaires à une certification ;

10° l'article 56, paragraphe 8, du règlement (UE) n° 2019/881 précité, en n'informant pas l'ILNAS ou l'organisme d'évaluation de la conformité de vulnérabilités ou d'irrégularités susceptibles d'avoir une incidence sur son respect des exigences liées à la certification.

(2) L'Administration de l'enregistrement, des domaines et de la TVA est chargée du recouvrement des amendes qui lui sont communiquées par le directeur de l'administration compétente. Le recouvrement est poursuivi comme en matière d'enregistrement.

(3) Les décisions d'infliger une amende administrative en vertu du présent article sont susceptibles d'un recours en réformation à introduire devant le tribunal administratif, dans le délai de trois mois à compter de la notification.

Art. 10. Sanctions administratives à l'encontre de titulaires de certificats de cybersécurité au niveau d'assurance dit « substantiel »

(1) Le directeur de l'ILNAS peut infliger une amende administrative de 250 euros à 25 000 euros aux titulaires de certificats de cybersécurité européens au niveau d'assurance dit « substantiel » qui enfreignent :

1° les articles 55, paragraphe 1er, lettres a), b), c) ou d), ou 55, paragraphe 2, du règlement (UE) n° 2019/881 précité, en ne mettant les informations supplémentaires spécifiées dans le schéma européen de certification de cybersécurité pas à disposition du public ou en ne les mettant pas à jour ;

2° les articles 52, paragraphe 2, et 54, paragraphe 1er, lettre d), du règlement (UE) n° 2019/881 précité, en publiant des informations par rapport à leur certification sans spécifier le niveau d'assurance ;

3° les dispositions du schéma européen de certification de cybersécurité concernant l'utilisation des labels et des marques conformément à l'article 54, paragraphe 1er, lettre i), du règlement (UE) n° 2019/881 précité ;

4° les dispositions du schéma européen de certification de cybersécurité concernant son champ d'application relatives à l'article 54, paragraphe 1er, lettre a), du règlement (UE) n° 2019/881 précité, en ne mettant pas ces informations à disposition du public ;

5° les dispositions du schéma européen de certification de cybersécurité concernant le format ou le contenu des certificats de cybersécurité européens conformément à l'article 54, paragraphe 1er, lettre p), du règlement (UE) n° 2019/881 précité ;

6° les dispositions du schéma européen de certification de cybersécurité concernant la période de disponibilité de la documentation technique ou de toutes les autres informations pertinentes qui sont mises à disposition par le fabricant ou le fournisseur de produits TIC, services TIC ou processus TIC, conformément aux articles 53, paragraphe 3, et 54, paragraphe 1er, lettre q), du règlement (UE) n° 2019/881 précité ;

7° les dispositions du schéma européen de certification de cybersécurité concernant la durée maximale de validité des certificats conformément à l'article 54, paragraphe 1er, lettre r), du règlement (UE) n° 2019/881 précité ;

8° l'article 56, paragraphe 7, du règlement (UE) n° 2019/881 précité, en ne mettant pas à disposition de l'ILNAS ou de l'organisme d'évaluation de la conformité les informations nécessaires à une certification ;

9° l'article 56, paragraphe 8, du règlement (UE) n° 2019/881 précité, en n'informant pas l'ILNAS ou l'organisme d'évaluation de la conformité de vulnérabilités ou d'irrégularités susceptibles d'avoir une incidence sur son respect des exigences liées à la certification.

(2) Le directeur de l'ILNAS peut infliger une amende administrative de 251 euros jusqu'à 50 000 euros aux titulaires de certificats de cybersécurité européen, au niveau d'assurance dit « substantiel » qui enfreignent les dispositions du schéma européen de certification de cybersécurité concernant le traitement des vulnérabilités de cybersécurité non détectées précédemment conformément aux articles 54, paragraphe 1er, lettre m), et 56, paragraphe 8, du règlement (UE) n° 2019/881 précité.

(3) L'Administration de l'enregistrement, des domaines et de la TVA est chargée du recouvrement des amendes qui lui sont communiquées par le directeur de l'administration compétente. Le recouvrement est poursuivi comme en matière d'enregistrement.

(4) Les décisions d'infliger une amende administrative en vertu du présent article sont susceptibles d'un recours en réformation à introduire devant le tribunal administratif, dans le délai de trois mois à compter de la notification.

Art. 11. Sanctions administratives à l'encontre de titulaires de certificats de cybersécurité au niveau d'assurance dit « élevé »

(1) Le directeur de l'ILNAS peut infliger une amende administrative de 250 euros à 25 000 euros aux titulaires de certificats de cybersécurité européens au niveau d'assurance dit « élevé » qui enfreignent :

1° les articles 55, paragraphe 1er, lettres a), b), c) ou d), ou 55, paragraphe 2, du règlement (UE) n° 2019/881 précité, en ne mettant les informations supplémentaires spécifiées dans le schéma européen de certification de cybersécurité pas à disposition du public ou en ne les mettant pas à jour ;

2° les articles 52, paragraphe 2, et 54, paragraphe 1er, lettre d), du règlement (UE) n° 2019/881 précité, en publiant des informations par rapport à leur certification sans spécifier le niveau d'assurance ;

3° les dispositions du schéma européen de certification de cybersécurité concernant l'utilisation des labels et des marques conformément à l'article 54, paragraphe 1er, lettre i), du règlement (UE) n° 2019/881 précité ;

4° les dispositions du schéma européen de certification de cybersécurité concernant son champ d'application relatives à l'article 54, paragraphe 1er, lettre a), du règlement (UE) n° 2019/881 précité, en ne mettant pas ces informations à disposition du public.

(2) Le directeur de l'ILNAS peut infliger une amende administrative de 251 euros jusqu'à 500 000 euros aux titulaires de certificats de cybersécurité européens, au niveau d'assurance dit « élevé », qui enfreignent :

1° les dispositions du schéma européen de certification de cybersécurité concernant le format ou le contenu des certificats de cybersécurité européens conformément à l'article 54, paragraphe 1er, lettre p), du règlement (UE) n° 2019/881 précité ;

2° les dispositions du schéma européen de certification de cybersécurité concernant la période de disponibilité de la documentation technique ou de toutes les autres informations pertinentes qui sont mises à disposition par le fabricant ou le fournisseur de produits TIC, services TIC ou processus TIC, conformément aux articles 53, paragraphe 3, et 54, paragraphe 1er, lettre q), du règlement (UE) n° 2019/881 précité ;

3° les dispositions du schéma européen de certification de cybersécurité concernant le traitement des vulnérabilités de cybersécurité non détectées précédemment conformément aux articles 54, paragraphe 1er, lettre m), et 56, paragraphe 8, du règlement (UE) n° 2019/881 précité ;

4° les dispositions du schéma européen de certification de cybersécurité concernant la durée maximale de validité des certificats conformément à l'article 54, paragraphe 1er, lettre r), du règlement (UE) n° 2019/881 précité ;

5° l'article 56, paragraphe 7, du règlement (UE) n° 2019/881 précité, en ne mettant pas à disposition de l'ILNAS ou de l'organisme d'évaluation de la conformité les informations nécessaires à une certification ;

6° l'article 56, paragraphe 8, du règlement (UE) n° 2019/881 précité, en n'informant pas l'ILNAS ou l'organisme d'évaluation de la conformité de vulnérabilités ou d'irrégularités susceptibles d'avoir une incidence sur son respect des exigences liées à la certification.

(3) L'Administration de l'enregistrement, des domaines et de la TVA est chargée du recouvrement des amendes qui lui sont communiquées par le directeur de l'administration compétente. Le recouvrement est poursuivi comme en matière d'enregistrement.

(4) Les décisions d'infliger une amende administrative en vertu du présent article sont susceptibles d'un recours en réformation à introduire devant le tribunal administratif, dans le délai de trois mois à compter de la notification.

Art. 12. Sanctions administratives à l'encontre d'organismes d'évaluation de la conformité

(1) Le directeur de l'ILNAS peut infliger une amende administrative de 250 euros à 25 000 euros aux organismes d'évaluation de la conformité qui certifient au niveau d'assurance dit « élémentaire » et qui enfreignent :

1° l'article 52, paragraphe 5, du règlement (UE) n° 2019/881 précité, en n'appliquant pas les activités d'évaluation appropriées lors d'une certification ;

2° l'article 56, paragraphe 4, du règlement (UE) n° 2019/881 précité, en ne respectant pas, lors de leur certification, les critères figurant dans les schémas de certification tels que définis dans l'article 54, paragraphe 1er, lettres a), d), f), g), j), k), l), n) ;

3° l'article 63, paragraphes 1er ou 2, du règlement (UE) n° 2019/881 précité, en n'acceptant pas ou ne traitant pas les réclamations en rapport avec un certificat de cybersécurité européen délivré par lui-même ;

4° l'annexe du règlement (UE) n° 2019/881 précité, en ne respectant pas les exigences auxquelles doivent satisfaire les organismes d'évaluation de la conformité telles que spécifiées ;

5° l'article 54, paragraphe 1er, lettre i), du règlement (UE) n° 2019/881 précité et les dispositions du schéma européen de certification de cybersécurité en délivrant des certificats non conformes ;

6° l'article 56, paragraphe 5, du règlement (UE) n° 2019/881 précité ou l'article 56, paragraphe 6, en octroyant, renouvelant ou en retirant des certificats du schéma européen de certification de cybersécurité sans avoir le mandat ou sans disposer de l'accréditation requise.

(2) Le directeur de l'ILNAS peut infliger une amende administrative de 251 euros jusqu'à 50 000 euros aux organismes d'évaluation de la conformité qui certifient au niveau d'assurance dit « substantiel » ou « élevé » et qui enfreignent l'article 63, paragraphes 1er et 2, du règlement (UE) n° 2019/881 précité, en n'acceptant pas ou ne traitant pas les réclamations en rapport avec un certificat de cybersécurité européen délivré par lui-même.

(3) Le directeur de l'ILNAS peut infliger une amende administrative de 251 euros jusqu'à 250 000 euros aux organismes d'évaluation de la conformité qui certifient au niveau d'assurance « substantiel » et qui enfreignent :

1° l'article 52, paragraphe 6, du règlement (UE) n° 2019/881 précité, en n'appliquant pas les activités d'évaluation appropriées lors d'une certification ;

2° l'article 56, paragraphe 4, du règlement (UE) n° 2019/881 précité, en ne respectant pas, lors de leur certification, les critères figurant dans les schémas de certification tels que définis dans l'article 54, paragraphe 1er, lettres a), d), f), g), j), k), l), n) ;

3° l'article 60, paragraphe 1er, du règlement (UE) n° 2019/881 précité, en octroyant, renouvelant ou en retirant des certificats du schéma européen de certification de cybersécurité sans avoir été accrédité ;

4° l'annexe du règlement (UE) n° 2019/881 précité, en ne respectant pas les exigences auxquelles doivent satisfaire les organismes d'évaluation de la conformité telles que spécifiées ;

5° l'article 54, paragraphe 1er, lettre i), du règlement (UE) n° 2019/881 précité et les dispositions du schéma européen de certification de cybersécurité en délivrant des certificats non conformes.

(4) Le directeur de l'ILNAS peut infliger une amende administrative de 251 euros jusqu'à 500 000 euros aux organismes d'évaluation de la conformité qui certifient au niveau d'assurance dit « élevé » et qui enfreignent :

1° l'article 52, paragraphe 7, du règlement (UE) n° 2019/881 précité, en n'appliquant pas les activités d'évaluation appropriées lors d'une certification ;

2° l'article 56, paragraphe 5, du règlement (UE) n° 2019/881 précité ou l'article 56, paragraphe 6, en octroyant, renouvelant ou en retirant des certificats du schéma européen de certification de cybersécurité sans avoir le mandat ;

3° l'annexe du règlement (UE) n° 2019/881 précité, en ne respectant pas les exigences auxquelles doivent satisfaire les organismes d'évaluation de la conformité telles que spécifiées ;

4° l'article 54, paragraphe 1er, lettre i), du règlement (UE) n° 2019/881 précité et les dispositions du schéma européen de certification de cybersécurité en délivrant des certificats non conformes.

(5) L'Administration de l'enregistrement, des domaines et de la TVA est chargée du recouvrement des amendes qui lui sont communiquées par le directeur de l'administration compétente. Le recouvrement est poursuivi comme en matière d'enregistrement.

(6) Les décisions d'infliger une amende administrative en vertu du présent article sont susceptibles d'un recours en réformation à introduire devant le tribunal administratif, dans le délai de trois mois à compter de la notification.

Art. 13. Sanctions pénales

Sont punis d'une amende de 251 euros jusqu'à 500 000 euros et d'une peine d'emprisonnement de huit jours à cinq ans ou d'une de ces peines seulement les titulaires de certificats de cybersécurité européens et les émetteurs de déclarations de conformité de l'Union européenne qui enfreignent :

1° l'article 58, paragraphe 8, lettre a), du règlement (UE) n° 2019/881 précité, en ne mettant pas à disposition de l'ILNAS toute information dont il a besoin pour l'exécution de ses tâches ;

2° l'article 58, paragraphe 8, lettre b), du règlement (UE) n° 2019/881 précité, en entravant les enquêtes de l'ILNAS.

Chapitre 5 – Dispositions modificatives

Art. 14. Modification de la loi modifiée du 4 juillet 2014 portant réorganisation de l'ILNAS

La loi modifiée du 4 juillet 2014 portant réorganisation de l'ILNAS est modifiée comme suit :

1° Dans l'ensemble de la loi, les termes « département de la confiance numérique » sont remplacés par les termes « Organisme luxembourgeois de la confiance numérique ».

2° A l'article 4, paragraphe 1er, point 5°, le point final est remplacé par un point-virgule et un point 6° nouveau est ajouté *in fine*, libellé comme suit :

« 6° à faire fonction d'Autorité nationale de certification de cybersécurité responsable des tâches de supervision au sens de l'article 58 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 responsable des tâches de certification au sens de l'article 56, paragraphe 6, du règlement (UE) n° 2019/881 précité. »

Luxembourg, le 5 décembre 2024

Le Président,
Carole HARTMANN

Le Rapporteur,
Guy ARENDT

Impression: CTIE – Division Imprimés et Fournitures de bureau