N° 8132²

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

* * *

AMENDEMENTS PARLEMENTAIRES

DEPECHE DU PRESIDENT DE LA CHAMBRE DES DEPUTES AU PRESIDENT DU CONSEIL D'ETAT

(11.4.2024)

Monsieur le Président,

J'ai l'honneur de vous soumettre ci-après des amendements au projet de loi sous rubrique, adoptés par la Commission de l'Economie, des PME, de l'Energie, de l'Espace et du Tourisme (ci-après « la commission »).

Je joins en annexe, à toutes fins utiles, un texte coordonné du projet de loi qui reprend toutes les modifications effectuées (ajouts figurant en caractères soulignés, suppressions en barré double) pour donner suite à l'avis du Conseil d'Etat.

*

REMARQUES PRELIMINAIRES

Dans ses considérations générales, le Conseil d'Etat exprime une certaine insatisfaction face au choix des auteurs du projet de loi de mettre en œuvre dans un dispositif légal autonome le règlement (UE) n° 2019/881 cité sous rubrique. Il aurait préféré voir les auteurs intégrer ces dispositions directement dans la loi modifiée du 4 juillet 2014 portant réorganisation de l'ILNAS. Cette préférence, de voir réunies toutes les missions de cette administration dans un seul et même texte, est à plusieurs égards parfaitement compréhensible. Or, compte tenu de l'urgence de cette mise en œuvre, ledit règlement étant déjà d'application, la commission juge le moment peu propice à une telle entreprise.

Quant à la préoccupation du Conseil d'Etat concernant 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).

La commission signale encore qu'elle 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. ».

*

AMENDEMENTS

Amendement 1er visant l'article 1er

Libellé :

« L'Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services, ~~(~~ci-après « ILNAS »~~)~~, est désigné comme ~~a~~Autorité nationale de certification de cybersécurité ~~(ci après « autorité nationale »)~~ 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, ci-après « règlement (UE) n° 2019/881 » ~~responsable des tâches de supervision~~ et responsable des tâches de certification au sens de l'article 56, paragraphe 6, du règlement (UE) n° 2019/881. »

Commentaire :

La commission a précisé le libellé de l'article 1er dans le sens des observations d'ordre légistique exprimées par le 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.

Amendement 2 visant l'article 3, paragraphe 2

Libellé :

« (2) Le comité a les missions suivantes :

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

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

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

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

5° ~~e)~~informer les parties prenantes concernées notamment 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, ~~point~~ lettre c), du règlement (UE) n° 2019/881 ;

6° ~~f)échanger des informations sur les évolutions dans le domaine de la cybersécurité~~ proposer au ministre, par schéma de certification, une liste de critères qui doivent être remplis pour autoriser, en application de l'article 56, paragraphe 6, lettre a), du règlement (UE) n° 2019/881, une certification d'un produit, service ou processus au niveau d'assurance dit « élevé ». Parmi ces critères sont notamment les secteurs cibles dans lesquels des certifications peuvent être autorisées. »

Commentaire :

Le paragraphe 2 de l'article 3 arrête les missions du Comité national de certification de cybersécurité.

Tandis que la modification 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)[1] vise à faire droit à l'observation afférente du Conseil d'Etat.

Le principal amendement 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 ».

---

1 Le mode d'énumération (lettres au lieu de chiffres) est également à adapter afin de le conformer aux règles légistiques.

Amendement 3 visant l'article 5, paragraphe 1er

Libellé :

« (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 européens donnent accès à l'~~a~~Autorité nationale de certification de cybersécurité ~~de~~ à toute ~~information,~~ document, toute personne, tout équipement et tout local dont elle a besoin pour pouvoir assurer ~~sa~~ ses tâches, ~~de supervision~~ en complément à l'article 58, paragraphe 8, lettre a), du règlement (UE) n° 2019/881. »

Commentaire :

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. ».

Afin de lever cette opposition formelle, la commission propose donc 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.

Amendement 4 visant l'article 5, ajout d'un paragraphe 3

Libellé :

« (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. »

Commentaire :

Constatant que le projet de loi sanctionne également pénalement le fait d'entraver les enquêtes de l'autorité nationale, le Conseil d'Etat souligne 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. » Il 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, reprenant la disposition à laquelle le Conseil d'Etat renvoie, la commission entend faire droit à son avis.

Amendement 5 visant l'article 7, suppression des paragraphes 1er et 3

Libellé :

« ~~(1) L'organisme d'évaluation de la conformité qui souhaite certifier des produits TIC, des services TIC et processus TIC, dans le cadre d'un schéma européen de certification de cybersécurité,~~

~~doit être accrédité au sens de l'article 60 du règlement (UE) n° 2019/881 et répondre aux exigences définies dans l'Annex e du règlement (UE) n° 2019/881.~~

(~~2~~1) L'organisme d'évaluation de la conformité accrédité au sens de l'article 60 du règlement (UE) n° 2019/881~~, en~~ informe, dans un délai de soixante-douze heures, l'~~a~~Autorité nationale de certification de cybersécurité de son accréditation.

~~(3) L'organisme d'évaluation de la conformité doit se soumettre au contrôle, par l'autorité nationale, des exigences spécifiques ou supplémentaires qui peuvent être définies dans les schémas européens de certification de cybersécurité, en application de l'article 54, paragraphe 1, point f) du règlement (UE) n° 2019/881, aux fins de notification et de supervision.~~ »

Commentaire :

La commission supprime le premier paragraphe, considéré par le 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 supprime également le paragraphe 3. Ce paragraphe se borne à reprendre une disposition afférente du règlement (UE) n° 2019/881, règlement qui est d'application directe.

Amendement 6 visant l'article 8, paragraphes 1er à 7

Libellé :

« (1) L'~~a~~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, ~~à la Commission européenne tout organisme d'évaluation de la conformité accrédité,~~ et le cas échéant, autorisé au sens de l'article 58, paragraphe 7, ~~point~~ 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.

L'~~a~~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 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, 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, qui émet de telles déclarations, telles que définies à l'article 53 du règlement (UE) n° 2019/881, 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.

(~~2~~3) Si l'~~a~~Autorité nationale de certification de cybersécurité constate ~~que les activités d'un organisme d'évaluation de la conformité qui émet des certificats~~ qu'un titulaire de certificat de cybersécurité ~~européens~~ au niveau d'assurance dit « élémentaire » ~~et « substantiel »~~, tel~~s~~ que défini~~s~~ ~~dans~~ à l'article 52 du règlement (UE) n° 2019/881, ~~n'est pas conforme aux exigences du règlement (UE) n° 2019/881, des actes d'exécution pris en son exécution, des schémas européens de certification de cybersécurité correspondants et à la présente loi, elle invite l'organisme d'évaluation de la conformité à se conformer à ces exigences~~ 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. ~~Si, p~~Passé ce délai, ~~l'organisme d'évaluation de la conformité ne s'est pas conformé à ces exigences~~, l'~~a~~Autorité nationale de certification de cybersécurité peut appliquer ~~des~~

les sanctions administratives afférentes prévues à l'article 9 ~~de la présente loi, respectivement dénonce les infractions par rapport à l'article 10 de la présente loi~~.

(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, 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, 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.

(~~3~~6) Si l'~~a~~Autorité nationale de certification de cybersécurité constate ~~que les activités d'un~~ qu'un organisme d'évaluation de la conformité~~, tel que défini dans l'article 56 paragraphe 6 a) ou b) du règlement (UE) n° 2019/881,~~ qui émet des certificats de cybersécurité européens aux niveaux d'assurance ~~dit « élevé »,~~ tels que définis dans l'article 52 du règlement (UE) n° 2019/881 précité, ~~ne sont pas conformes aux exigences du règlement (UE) n° 2019/881, des actes d'exécution pris en son exécution, des schémas européens de certification de cybersécurité correspondants et à la présente loi~~ a un comportement visé à l'article 14 et sanctionné par ce même article, elle invite l'organisme d'évaluation de la conformité à ~~se conformer à ces exigences~~ y remédier, dans les délais qu'elle détermine. Si, passé ce délai, l'organisme d'évaluation de la conformité ~~ne s'est pas conformé à ces exigences~~ n'y a pas remédié, l'~~a~~Autorité nationale de certification de cybersécurité peut ~~décider des~~ appliquer les sanctions administratives afférentes prévues à l'article ~~9 de la présente loi, respectivement dénonce les infractions par rapport à l'article 10 de la présente loi~~12.

~~(4) Si l'autorité nationale constate que les activités d'un titulaire de certificats ou d'un émetteur d'une déclaration de conformité ne sont pas conformes aux exigences du règlement (UE) n° 2019/881, des actes d'exécution pris en son exécution, des schémas européens de certification de cybersécurité correspondants et à la présente loi, elle invite le titulaire de certificats respectivement l'émetteur d'une déclaration de conformité à se conformer, dans les délais qu'elle détermine. Si, passé ce délai, le titulaire de certificats ou l'émetteur d'une déclaration de conformité ne s'est pas conformé à ces exigences, l'autorité nationale peut leur appliquer des sanctions administratives prévues à l'article 9 de la présente loi, respectivement dénonce les infractions par rapport à l'article 10 de la présente loi.~~

~~(5) En cas de constatation 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, l'autorité nationale peut en informer à telles fins que de droit les ministères compétents. Les rapports établis à l'attention de l'autorité nationale peuvent être communiqués à ces autorités, dans la mesure où le titulaire de certificats et l'émetteur de déclarations de conformité en a reçu communication par l'autorité nationale.~~

(~~4~~7) L'~~a~~Autorité nationale de certification de cybersécurité peut procéder à tout moment~~, aussi sur demande dûment justifiée de personnes intéressées,~~ 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'~~a~~Autorité nationale de certification de cybersécurité peut avoir recours à des experts externes pour effectuer ces vérifications. Les frais d'experts sont ~~couverts par les~~ refacturés aux titulaires de certificats de cybersécurité européens ~~de cybersécurité européens~~, ~~les~~ aux émetteurs de déclarations de conformité de l'Union européenne et ~~les~~ aux organismes d'évaluation de la conformité européens.

(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. Le barème tarifaire, approuvé par le ministre, est publié sur le site électronique installé à cet effet par l'ILNAS.

(~~7~~9) L'~~a~~Autorité nationale de certification de cybersécurité peut collaborer avec d'autres autorités compétentes dans un autre Etat membre pour exécuter ses tâches de supervision. ~~Si l'autorité nationale rencontre des difficultés dans l'exercice de ses pouvoirs de contrôle, elle peut requérir l'assistance de la Police grand-ducale en vertu des dispositions contenues aux articles 27 et ss dans la loi du 18 juillet 2018 sur la Police Grand-Ducale.~~ »

Commentaire :

L'article 8 du projet de loi a été retravaillé de fond en comble, non seulement en raison des observations exprimées directement à son égard par le 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 et les sanctions pénales ont été abandonnées.

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 rapporte 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 également 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.

Amendement 7 ajoutant les articles 9 à 12

Libellé :

« **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 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 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 ;

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 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 ;

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 ;

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 doivent être 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 ;

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 ;

9° l'article 56, paragraphe 7, du règlement (UE) n° 2019/881 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 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 ;

11° l'article 58, paragraphe 8, lettre a°, du règlement (UE) n° 2019/881 en ne mettant pas à disposition de l'ILNAS toute information dont elle a besoin pour l'exécution de ses tâches ;

12° l'article 58, paragraphe 8, lettre b°, du règlement (UE) n° 2019/881 en entravant les enquêtes de l'ILNAS.

(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 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 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 ;

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 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 ;

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 doivent être 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 ;

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 ;

8° l'article 56, paragraphe 7, du règlement (UE) n° 2019/881 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 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 ;

10° l'article 58, paragraphe 8, lettre a°, du règlement (UE) n° 2019/881 en ne mettant pas à disposition de l'ILNAS toute information dont elle a besoin pour l'exécution de ses tâches ;

11° l'article 58, paragraphe 8, lettre b°, du règlement (UE) n° 2019/881 en entravant les enquêtes de l'ILNAS.

(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 :

1° 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 ;

2° l'article 58, paragraphe 8, lettre a°, du règlement (UE) n° 2019/881 en ne mettant pas à disposition de l'ILNAS toute information dont elle a besoin pour l'exécution de ses tâches ;

3° l'article 58, paragraphe 8, lettre b°, du règlement (UE) n° 2019/881 en entravant les enquêtes de l'ILNAS.

(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 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, 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 ;

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 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 ;

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 doivent être 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 ;

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 ;

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 ;

5° l'article 56, paragraphe 7, du règlement (UE) n° 2019/881 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 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 ;

7° l'article 58, paragraphe 8, lettre a°, du règlement (UE) n° 2019/881 en ne mettant pas à disposition de l'ILNAS toute information dont elle a besoin pour l'exécution de ses tâches ;

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

(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 européens qui certifient au niveau d'assurance dit « élémentaire » et qui enfreignent :

1° l'article 52, paragraphe 5 du règlement (UE) n° 2019/881 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 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 58, paragraphe 8, lettre a°, du règlement (UE) n° 2019/881 en ne mettant pas à disposition de l'ILNAS toute information dont elle a besoin pour l'exécution de ses tâches ;

4° l'article 58, paragraphe 8, lettre b°, du règlement (UE) n° 2019/881 en entravant les enquêtes de l'ILNAS ;

5° l'article 63, paragraphes 1er ou 2, du règlement (UE) n° 2019/881 en n'acceptant pas ou ne traitant pas les réclamations en rapport avec un certificat de cybersécurité européen délivré par lui-même ;

6° l'annexe du règlement (UE) n° 2019/881 en ne respectant pas les exigences auxquelles doivent satisfaire les organismes d'évaluation de la conformité telles que spécifiées ;

7° l'article 54, paragraphe 1er, lettre i°, du règlement (UE) n° 2019/881 et les dispositions du schéma européen de certification de cybersécurité en délivrant des certificats non conformes ;

8° l'article 56, paragraphe 5, du règlement (UE) n° 2019/881 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 européens 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, 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 européens qui certifient au niveau d'assurance « substantiel » et qui enfreignent :

1° l'article 52, paragraphe 6, du règlement (UE) n° 2019/881 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 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 en octroyant, renouvelant ou en retirant des certificats du schéma européen de certification de cybersécurité sans avoir été accrédité ;

4° l'article 58, paragraphe 8, lettre a°, du règlement (UE) n° 2019/881 en ne mettant pas à disposition de l'ILNAS toute information dont elle a besoin pour l'exécution de ses tâches ;

5° l'article 58, paragraphe 8, lettre b°, du règlement (UE) n° 2019/881 en entravant les enquêtes de l'ILNAS ;

6° l'annexe du règlement (UE) n° 2019/881 en ne respectant pas les exigences auxquelles doivent satisfaire les organismes d'évaluation de la conformité telles que spécifiées ;

7° l'article 54, paragraphe 1er, lettre i°, du règlement (UE) n° 2019/881 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 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 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'article 58, paragraphe 8, lettre a°, du règlement (UE) n° 2019/881 en ne mettant pas à disposition de l'ILNAS toute information dont elle a besoin pour l'exécution de ses tâches ;

4° l'article 58, paragraphe 8, lettre b°, du règlement (UE) n° 2019/881 en entravant les enquêtes de l'ILNAS ;

5° l'annexe du règlement (UE) n° 2019/881 en ne respectant pas les exigences auxquelles doivent satisfaire les organismes d'évaluation de la conformité telles que spécifiées ;

6° l'article 54, paragraphe 1er, lettre i°, du règlement (UE) n° 2019/881 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. *»*

Commentaire :

Dans son avis, le Conseil d'Etat s'oppose formellement au double régime répressif prévu, administratif et pénal.

Le Conseil d'Etat constate, en effet, 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. ».

En réaction, la commission a limité le régime répressif à des sanctions administratives.

Les anciens paragraphes 2 à 5 de l'ancien article 9 ont été supprimés.

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).

Pour les titulaires de certificats de cybersécurité aux niveaux d'assurance dits « substantiel » et « élevé » 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.

L'article visant les organismes d'évaluation de la conformité a été restructuré afin de refléter l'impact potentiel des infractions commises.

Amendement 8 supprimant l'article 10

Libellé :

« ~~**Art. 10. Sanctions pénales**~~

~~(1) Sont punis d'une amende de 251 euros jusqu'à 25 000 euros et d'une peine d'emprisonnement de huit jours à 6 mois ou d'une de ces peines seulement les titulaires de certificats de cybersécurité européen, au niveau d'assurance dit 'substantiel', qui enfreignent :~~

(...)

~~(6) Est puni d'une amende de 251 euros à 500 000 euros et d'une peine d'emprisonnement de huit jours à cinq ans ou d'une de ces peines seulement toute personne qui ne s'est pas conformée au secret professionnel prévu par l'article 6, paragraphe 1er.~~ »

Commentaire :

Compte tenu de l'opposition formelle du Conseil d'Etat, le régime répressif prévu a été limité à un dispositif de sanctions administratives.

L'ancien article 10, regroupant les sanctions pénales initialement prévues, a été supprimé.

La commission renvoie à son amendement 7 visant les articles 9 à 12 nouveaux.

*

J'envoie copie de la présente à la Ministre déléguée auprès du Premier ministre, chargée des Relations avec le Parlement, avec prière de transmettre les amendements aux instances à consulter.

Veuillez agréer, Monsieur le Président, l'expression de ma considération très distinguée.

Le Président de la Chambre des Députés,
Claude WISELER

*

TEXTE COORDONNE

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

~~CHAPITRE~~ 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 ~~a~~Autorité nationale de certification de cybersécurité ~~(ci après « autorité nationale »)~~ 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, ci-après « règlement (UE) n° 2019/881 » ~~responsable des tâches de supervision~~ et responsable des tâches de certification au sens de l'article 56, paragraphe 6, du règlement (UE) n° 2019/881.

Art. 2. Groupe européen de certification de cybersécurité

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

Art. 3. Comité national de certification de cybersécurité

(1) Un ~~c~~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° ~~a)aviser sur~~ conseiller le ministre en ce qui concerne le programme de travail glissant de l'Union européenne pour la certification européenne de cybersécurité ;

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

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

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

5° ~~e)~~informer les parties prenantes concernées notamment 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, ~~point~~ lettre c), du règlement (UE) n° 2019/881 ;

6° ~~f)échanger des informations sur les évolutions dans le domaine de la cybersécurité~~ proposer au ministre, par schéma de certification, une liste de critères qui doivent être remplis pour autoriser, en application de l'article 56, paragraphe 6, lettre a), du règlement (UE) n° 2019/881, une certification d'un produit, service ou processus au niveau d'assurance dit « élevé ». Parmi ces critères sont notamment les secteurs cibles dans lesquels des certifications peuvent être autorisées.

~~CHAPITRE~~ 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'~~a~~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 européens donnent accès à l'~~a~~Autorité nationale de certification de cybersécurité ~~de~~ à toute~~ information,~~ document, toute personne, tout équipement et tout local dont elle a besoin pour pouvoir assurer ~~sa~~ ses tâches, ~~de supervision~~ en complément à l'article 58, paragraphe 8, lettre a), du règlement (UE) n° 2019/881.

(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 européens informent l'~~a~~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.

(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 – Obligations au secret professionnel.~~

~~**Art. 6. Secret professionnel**~~

~~(1) Toute personne chargée ou ayant été chargée de procéder à des audits par l'autorité nationale auprès des fabricants ou fournisseurs de produits TIC, services TIC et processus TIC est tenue au secret professionnel et passible des peines prévues à l'article 10, paragraphe 6 de la présente loi.~~

~~(2) L'obligation au secret cesse lorsque la révélation d'un renseignement est autorisée ou imposée par ou en vertu d'une disposition législative, même antérieure à la présente loi.~~

~~(3) L'obligation au secret professionnel n'existe pas à l'égard de l'autorité nationale et de l'organisme national d'accréditation agissant dans le cadre de ses missions et compétences légales.~~

Section ~~3~~2 – Les organismes d'évaluation de la conformité~~.~~

Art. ~~7~~6. Obligations des organismes d'évaluation de la conformité

~~(1) L'organisme d'évaluation de la conformité qui souhaite certifier des produits TIC, des services TIC et processus TIC, dans le cadre d'un schéma européen de certification de cybersécurité, doit être accrédité au sens de l'article 60 du règlement (UE) n° 2019/881 et répondre aux exigences définies dans l'Annexe du règlement (UE) n° 2019/881.~~

(~~2~~1) L'organisme d'évaluation de la conformité accrédité au sens de l'article 60 du règlement (UE) n° 2019/881~~, en~~ informe, dans un délai de soixante-douze heures, l'~~a~~Autorité nationale de certification de cybersécurité de son accréditation.

~~(3) L'organisme d'évaluation de la conformité doit se soumettre au contrôle, par l'autorité nationale, des exigences spécifiques ou supplémentaires qui peuvent être définies dans les schémas européens de certification de cybersécurité, en application de l'article 54, paragraphe 1, point f) du règlement (UE) n° 2019/881, aux fins de notification et de supervision.~~

(~~4~~2) L'~~a~~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.

~~CHAPITRE~~ Chapitre 3 – L'~~a~~Autorité nationale de certification de cybersécurité~~.~~

Art. ~~8~~7. Rôle de l'~~a~~Autorité nationale de certification de cybersécurité

(1) L'~~a~~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, ~~à la Commission européenne tout organisme d'évaluation de la conformité accrédité,~~ et le cas échéant, autorisé au sens de l'article 58, paragraphe 7, ~~point~~ 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.

L'~~a~~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 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, 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, qui émet de telles déclarations, telles que définies à l'article 53 du règlement (UE) n° 2019/881, 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.

(~~2~~3) Si l'~~a~~Autorité nationale de certification de cybersécurité constate ~~que les activités d'un organisme d'évaluation de la conformité qui émet des certificats~~ qu'un titulaire de certificat de cybersécurité ~~européens~~ au niveau d'assurance dit « élémentaire » ~~et « substantiel »~~, tel~~s~~ que défini~~s dans~~ à l'article 52 du règlement (UE) n° 2019/881, ~~n'est pas conforme aux exigences du n° 2019/881, des actes d'exécution pris en son exécution, des schémas européens de certification de cybersécurité correspondants et à la présente loi, elle invite l'organisme d'évaluation de la conformité à se conformer à ces exigences~~ 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. ~~Si, p~~Passé ce délai, ~~l'organisme d'évaluation de la conformité ne s'est pas conformé à ces exigences~~, l'~~a~~Autorité nationale de certification de cybersécurité peut appliquer ~~des~~ les sanctions administratives afférentes prévues à l'article 9 ~~de la présente loi, respectivement dénonce les infractions par rapport à l'article 10 de la présente loi~~.

(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, 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, 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.

(~~3~~6) Si l'~~a~~Autorité nationale de certification de cybersécurité constate ~~que les activités d'un~~ qu'un organisme d'évaluation de la conformité~~, tel que défini dans l'article 56 paragraphe 6 a) ou b) du règlement (UE) n° 2019/881,~~ qui émet des certificats de cybersécurité européens aux niveaux d'assurance ~~dit « élevé »,~~ tels que définis dans l'article 52 du règlement (UE) n° 2019/881 précité, ~~ne sont pas conformes aux exigences du règlement (UE) n° 2019/881, des actes d'exécution pris en son exécution, des schémas européens de certification de cybersécurité correspondants et à la présente loi~~ a un comportement visé à l'article 14 et sanctionné par ce même article, elle invite l'organisme d'évaluation de la conformité à ~~se conformer à ces exigences~~ y remédier, dans les délais qu'elle détermine. Si, passé ce délai, l'organisme d'évaluation de la conformité ~~ne s'est pas conformé à ces exigences~~ n'y a pas remédié, l'~~a~~Autorité nationale de certification de cybersécurité peut ~~décider des~~ appliquer les sanctions administratives afférentes prévues à l'article ~~9 de la présente loi, respectivement dénonce les infractions par rapport à l'article 10 de la présente loi~~12.

~~(4) Si l'autorité nationale constate que les activités d'un titulaire de certificats ou d'un émetteur d'une déclaration de conformité ne sont pas conformes aux exig ences du règlement (UE) n° 2019/881, des actes d'exécution pris en son exécution, des schémas européens de certification de cybersécurité correspondants et à la présente loi, elle invite le titulaire de certificats respectivement l'émetteur d'une déclaration de conformité à se conformer, dans les délais qu'elle détermine. Si, passé ce délai, le titulaire de certificats ou l'émetteur d'une déclaration de conformité ne s'est pas conformé à ces exigences, l'autorité nationale peut leur appliquer des sanctions administratives prévues à l'article 9 de la présente loi, respectivement dénonce les infractions par rapport à l'article 10 de la présente loi.~~

~~(5) En cas de constatation 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, l'autorité nationale peut en informer à telles fins que de droit les ministères compétents. Les rapports établis à l'attention de l'autorité nationale peuvent être communiqués à ces autorités, dans la mesure où le titulaire de certificats et l'émetteur de déclarations de conformité en a reçu communication par l'autorité nationale.~~

(~~6~~7) L'~~a~~Autorité nationale de certification de cybersécurité peut procéder à tout moment~~, aussi sur demande dûment justifiée de personnes intéressées,~~ 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'~~a~~Autorité nationale de certification de cybersécurité peut avoir recours à des experts externes pour effectuer ces vérifications. Les frais d'experts sont ~~couverts par les~~ refacturés aux titulaires de certificats de cybersécurité européens ~~de cybersécurité européens~~, ~~les~~ aux émetteurs de déclarations de conformité de l'Union européenne et ~~les~~ aux organismes d'évaluation de la conformité européens.

(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. Le barème tarifaire, approuvé par le ministre, est publié sur le site électronique installé à cet effet par l'ILNAS.

(~~7~~9) L'~~a~~Autorité nationale de certification de cybersécurité peut collaborer avec d'autres autorités compétentes dans un autre Etat membre pour exécuter ses tâches de supervision. ~~Si l'autorité nationale rencontre des difficultés dans l'exercice de ses pouvoirs de contrôle, elle peut requérir l'assistance de la Police grand-ducale en vertu des dispositions contenues aux articles 27 et ss dans la loi du 18 juillet 2018 sur la Police Grand-Ducale.~~

(~~8~~10) L'~~a~~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~~ Chapitre 4 – Sanctions~~.~~

Art. ~~98~~. Sanctions administratives à l'encontre d'émetteurs de déclarations de conformité de l'Union européenne

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

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

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

4° ~~d)~~l'article 53, paragraphe 2, du règlement (UE) n° 2019/881 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, ~~point~~lettre j°, du règlement (UE) n° 2019/881 ;

5° ~~e)~~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, ~~point~~lettre l°, du règlement (UE) n° 2019/881 ;

6° ~~f)~~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, ~~point~~lettre m°, et 56, paragraphe 8, du règlement (UE) n° 2019/881 ;

7° ~~g)~~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, ~~point~~lettre p°, du règlement (UE) n° 2019/881 ;

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

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

10° ~~j)~~l'article 58, paragraphe 8, ~~point~~lettre a°, du règlement (UE) n° 2019/881 en ne mettant pas à disposition de l'ILNAS toute information dont elle a besoin pour l'exécution de ses tâches ;

11° ~~k)~~l'article 58, paragraphe 8, ~~point~~lettre b°, du règlement (UE) n° 2019/881~~,~~ en entravant les enquêtes de l'ILNAS.

~~(2) Le chef de l'administration de l'ILNAS peut infliger une amende administrative de 250 euros à 25.000 euros aux titulaires de certificats de cybersécurité européens qui enfreignent :~~

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

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

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

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

(3) Le chef de l'administration de l'ILNAS peut infliger une amende administrative de 250 euros à 25 000 euros aux titulaires de certificats de cybersécurité européens qui, au niveau d'assurance dit « élémentaire », 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, point m°, et 56, paragraphe 8, du règlement (UE) n° 2019/881.

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

a) 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, point p°, du règlement (UE) n°2019/881 ;

b) les disposition du schéma européen de certification de cybersécurité concernant la période de disponibilité de la documentation technique ou de toutes les autres informations pertinentes qui doivent être 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, point q°, du règlement (UE) n° 2019/881;

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

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

e) l'article 56, paragraphe 8, du règlement (UE) n° 2019/881, en n'informant pas l'ILNAS respectivement 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 ;

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

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

(5) Le chef de l'administration 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:

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

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

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

d) l'article 58, paragraphe 8, point b°, du règlement (UE) n° 2019/881 en entravant les enquêtes de l'ILNAS ;

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

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

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

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

(~~6~~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.

(~~7~~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 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 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 ;

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 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 ;

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 ;

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 doivent être 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 ;

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 ;

9° l'article 56, paragraphe 7, du règlement (UE) n° 2019/881 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 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 ;

11° l'article 58, paragraphe 8, lettre a°, du règlement (UE) n° 2019/881 en ne mettant pas à disposition de l'ILNAS toute information dont elle a besoin pour l'exécution de ses tâches ;

12° l'article 58, paragraphe 8, lettre b°, du règlement (UE) n° 2019/881 en entravant les enquêtes de l'ILNAS.

(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 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 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 ;

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 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 ;

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 doivent être 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 ;

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 ;

8° l'article 56, paragraphe 7, du règlement (UE) n° 2019/881 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 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 ;

10° l'article 58, paragraphe 8, lettre a°, du règlement (UE) n° 2019/881 en ne mettant pas à disposition de l'ILNAS toute information dont elle a besoin pour l'exécution de ses tâches ;

11° l'article 58, paragraphe 8, lettre b°, du règlement (UE) n° 2019/881 en entravant les enquêtes de l'ILNAS.

(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 :

1° 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 ;

2° l'article 58, paragraphe 8, lettre a°, du règlement (UE) n° 2019/881 en ne mettant pas à disposition de l'ILNAS toute information dont elle a besoin pour l'exécution de ses tâches ;

3° l'article 58, paragraphe 8, lettre b°, du règlement (UE) n° 2019/881 en entravant les enquêtes de l'ILNAS.

(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 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, 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 ;

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 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 ;

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 doivent être 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 ;

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 ;

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 ;

5° l'article 56, paragraphe 7, du règlement (UE) n° 2019/881 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 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 ;

7° l'article 58, paragraphe 8, lettre a°, du règlement (UE) n° 2019/881 en ne mettant pas à disposition de l'ILNAS toute information dont elle a besoin pour l'exécution de ses tâches ;

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

(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 européens qui certifient au niveau d'assurance dit « élémentaire » et qui enfreignent :

1° l'article 52, paragraphe 5 du règlement (UE) n° 2019/881 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 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 58, paragraphe 8, lettre a°, du règlement (UE) n° 2019/881 en ne mettant pas à disposition de l'ILNAS toute information dont elle a besoin pour l'exécution de ses tâches ;

4° l'article 58, paragraphe 8, lettre b°, du règlement (UE) n° 2019/881 en entravant les enquêtes de l'ILNAS ;

5° l'article 63, paragraphes 1er ou 2, du règlement (UE) n° 2019/881 en n'acceptant pas ou ne traitant pas les réclamations en rapport avec un certificat de cybersécurité européen délivré par lui-même ;

6° l'annexe du règlement (UE) n° 2019/881 en ne respectant pas les exigences auxquelles doivent satisfaire les organismes d'évaluation de la conformité telles que spécifiées ;

7° l'article 54, paragraphe 1er, lettre i°, du règlement (UE) n° 2019/881 et les dispositions du schéma européen de certification de cybersécurité en délivrant des certificats non conformes ;

8° l'article 56, paragraphe 5, du règlement (UE) n° 2019/881 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 européens 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, 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 européens qui certifient au niveau d'assurance « substantiel » et qui enfreignent :

1° l'article 52, paragraphe 6, du règlement (UE) n° 2019/881 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 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 en octroyant, renouvelant ou en retirant des certificats du schéma européen de certification de cybersécurité sans avoir été accrédité ;

4° l'article 58, paragraphe 8, lettre a°, du règlement (UE) n° 2019/881 en ne mettant pas à disposition de l'ILNAS toute information dont elle a besoin pour l'exécution de ses tâches ;

5° l'article 58, paragraphe 8, lettre b°, du règlement (UE) n° 2019/881 en entravant les enquêtes de l'ILNAS ;

6° l'annexe du règlement (UE) n° 2019/881 en ne respectant pas les exigences auxquelles doivent satisfaire les organismes d'évaluation de la conformité telles que spécifiées ;

7° l'article 54, paragraphe 1er, lettre i°, du règlement (UE) n° 2019/881 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 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 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'article 58, paragraphe 8, lettre a°, du règlement (UE) n° 2019/881 en ne mettant pas à disposition de l'ILNAS toute information dont elle a besoin pour l'exécution de ses tâches ;

4° l'article 58, paragraphe 8, lettre b°, du règlement (UE) n° 2019/881 en entravant les enquêtes de l'ILNAS ;

5° l'annexe du règlement (UE) n° 2019/881 en ne respectant pas les exigences auxquelles doivent satisfaire les organismes d'évaluation de la conformité telles que spécifiées ;

6° l'article 54, paragraphe 1er, lettre i°, du règlement (UE) n° 2019/881 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. 10. Sanctions pénales**~~

~~(1) Sont punis d'une amende de 251 euros jusqu'à 25 000 euros et d'une peine d'emprisonnement de huit jours à 6 mois ou d'une de ces peines seulement les titulaires de certificats de cybersécurité européen, au niveau d'assurance dit 'substantiel', qui enfreignent :~~

~~a) 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, point m°, et 56, paragraphe 8, du règlement (UE) n° 2019/881 ;~~

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

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

~~(2) Sont punis d'une amende de 251 euros jusqu'à 500 000 euros et d'une peine d'emprisonnement de huit jours à 5 ans ou d'une de ces peines seulement, les titulaires de certificats de cybersécurité européens , au niveau d'assurance dit 'élevé', qui enfreignent :~~

~~a) 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, point p°, du règlement (UE) n° 2019/881 ;~~

~~b) 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 doivent être 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, point q°, du règlement (UE) n° 2019/881;~~

~~c) 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, point m°, et 56, paragraphe 8, du règlement (UE) n° 2019/881 ;~~

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

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

f) l'article 56, paragraphe 8, du règlement (UE) n° 2019/881, en n'informant pas l'ILNAS respectivement 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 ;

g) l'article 58, paragraphe 8, point a°, du règlement (UE) n° 2019/881, en ne mettant pas à disposition de l'ILNAS toute information dont elle a besoin pour l'exécution de ses tâches.

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

(3) Sont punis d'une amende de 251 euros jusqu'à 25 000 euros et d'une peine d'emprisonnement de huit jours à 6 mois ou d'une de ces peines seulement aux organismes d'évaluation de la conformité européens 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, en n'acceptant pas respectivement ne traitant pas les réclamations en rapport avec un certificat de cybersécurité européen délivré par lui même.

(4) Sont punis d'une amende de 251 euros jusqu'à 250 000 euros et d'une peine d'emprisonnement de huit jours à 2 ans ou d'une de ces peines seulement les organismes d 'évaluation de la conformité européens qui certifient au niveau d'assurance 'substantiel', et enfreignent :

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

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

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

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

e) l'article 58, paragraphe 8, point b°, du règlement (UE) n° 2019/881 en entravant les enquêtes de l'ILNAS;

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

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

(5) Sont punis d'une amende de 251 euros jusqu'à 500 000 euros et d'une peine d'emprisonnement de huit jours à 5 ans ou d'une de ces peines seulement tous organismes d'évaluation de la conformité qui certifient au niveau d'assurance dit 'élevé' et qui enfreignent :

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

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

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

d) l'article 58, paragraphe 8, point b°, du règlement (UE) n° 2019/881 en entravant les enquêtes de l'ILNAS ;

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

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

(6) Est puni d'une amende de 251 euros à 500 000 euros et d'une peine d'emprisonnement de huit jours à cinq ans ou d'une de ces peines seulement toute personne qui ne s'est pas conformée au secret professionnel prévu par l'article 6, paragraphe 1er.

~~CLIAPITRE~~Chapitre 5 – Dispositions modificatives~~.~~

Art. ~~11~~13. 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, ~~au~~ point 5°, ~~de la même loi,~~ le point final est remplacé par un point-virgule et ~~à la fin du point 5°,~~ un ~~nouveau~~ point 6° nouveau ~~au libellé suivant est inséré~~ est ajouté *in fine*, libellé comme suit :

« 6° à ~~assumer les tâches~~ faire fonction d'~~a~~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), ci-après « règlement (UE) n° 2019/881 » et responsable des tâches de certification au sens de l'article 56, paragraphe 6, du règlement (UE) n° 2019/881. »

Impression: CTIE – Division Imprimés et Fournitures de bureau