Parlement européen
2019-2024

Document de séance

A9-0307/2023

26.10.2023

***I
RAPPORT

sur la proposition de règlement du Parlement européen et du Conseil modifiant le règlement (UE) 2019/881 en ce qui concerne les services de sécurité gérés (COM(2023)0208 – C9-0137/2023 – 2023/0108(COD))

Commission de l'industrie, de la recherche et de l'énergie

Rapporteure: Josianne Cutajar

Légende des signes utilisés

*	Procédure de consultation
***	Procédure d'approbation
***I	Procédure législative ordinaire (première lecture)
***II	Procédure législative ordinaire (deuxième lecture)
***III	Procédure législative ordinaire (troisième lecture)

(La procédure indiquée est fondée sur la base juridique proposée par le projet d'acte.)

Amendements à un projet d'acte

Amendements du Parlement présentés en deux colonnes

Les suppressions sont signalées par des ***italiques gras*** dans la colonne de gauche. Les remplacements sont signalés par des ***italiques gras*** dans les deux colonnes. Le texte nouveau est signalé par des ***italiques gras*** dans la colonne de droite.

Les première et deuxième lignes de l'en-tête de chaque amendement identifient le passage concerné dans le projet d'acte à l'examen. Si un amendement porte sur un acte existant, que le projet d'acte entend modifier, l'en-tête comporte en outre une troisième et une quatrième lignes qui identifient respectivement l'acte existant et la disposition de celui-ci qui est concernée.

Amendements du Parlement prenant la forme d'un texte consolidé

Les parties de textes nouvelles sont indiquées en ***italiques gras***. Les parties de texte supprimées sont indiquées par le symbole ▌ ou barrées. Les remplacements sont signalés en indiquant en ***italiques gras*** le texte nouveau et en effaçant ou en barrant le texte remplacé.
Par exception, les modifications de nature strictement technique apportées par les services en vue de l'élaboration du texte final ne sont pas marquées.

SOMMAIRE

Page

PROJET DE RÉSOLUTION LÉGISLATIVE DU PARLEMENT EUROPÉEN 5

EXPOSÉ DES MOTIFS 30

LETTRE DE LA COMMISSION DU MARCHÉ INTÉRIEUR ET DE LA PROTECTION DES CONSOMMATEURS.....32

PROCÉDURE DE LA COMMISSION COMPÉTENTE AU FOND 37

VOTE FINAL PAR APPEL NOMINAL EN COMMISSION COMPÉTENTE AU FOND ..38

PROJET DE RÉSOLUTION LÉGISLATIVE DU PARLEMENT EUROPÉEN

sur la proposition de règlement du Parlement européen et du Conseil modifiant le règlement (UE) 2019/881 en ce qui concerne les services de sécurité gérés (COM(2023)0208 – C9-0137/2023 – 2023/0108(COD))

(Procédure législative ordinaire: première lecture)

Le Parlement européen,

– vu la proposition de la Commission au Parlement européen et au Conseil (COM(2023)0208),

– vu l'article 294, paragraphe 2, et l'article 114 du traité sur le fonctionnement de l'Union européenne, conformément auxquels la proposition lui a été présentée par la Commission (C9-0137/2023),

– vu l'article 294, paragraphe 3, du traité sur le fonctionnement de l'Union européenne,

– vu l'avis du Comité économique et social européen du 13 juillet 2023[1],

– vu l'article 59 de son règlement intérieur,

– vu la lettre de la commission du marché intérieur et de la protection des consommateurs,

– vu le rapport de la commission de l'industrie, de la recherche et de l'énergie (A9-0307/2023),

1. arrête la position en première lecture figurant ci-après;

2. demande à la Commission de le saisir à nouveau, si elle remplace, modifie de manière substantielle ou entend modifier de manière substantielle sa proposition;

3. charge sa Présidente de transmettre sa position au Conseil et à la Commission ainsi qu'aux parlements nationaux.

[1] JO C 349 du 29.9.2023, p. 167.

Amendement 1

AMENDEMENTS DU PARLEMENT EUROPÉEN*

à la proposition de la Commission

2023/0108 (COD)

Proposition de

RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL

modifiant le règlement (UE) 2019/881 en ce qui concerne les services de sécurité gérés

(Texte présentant de l'intérêt pour l'EEE)

LE PARLEMENT EUROPÉEN ET LE CONSEIL DE L'UNION EUROPÉENNE,

vu le traité sur le fonctionnement de l'Union européenne, et notamment son article 114,

vu la proposition de la Commission européenne,

après transmission du projet d'acte législatif aux parlements nationaux,

vu l'avis du Comité économique et social européen[2],

vu l'avis du Comité des régions,

statuant conformément à la procédure législative ordinaire[3],

---

* Amendements: le texte nouveau ou modifié est signalé par des italiques gras; les suppressions sont signalées par le symbole ▌.

2 ***JO C 349 du 29.9.2023, p. 167.***

3 ***Position du Parlement européen du … (non encore parue au Journal officiel) et décision du Conseil du ….***

considérant ce qui suit:

(1) Le règlement (UE) 2019/881 du Parlement européen et du Conseil[4] fixe un cadre pour la mise en place de schémas européens de certification de cybersécurité dans le but de garantir un niveau adéquat de cybersécurité des produits ***des technologies de l'information et de la communication (***TIC***)***, services TIC et processus TIC dans l'Union, ainsi que dans le but d'éviter la fragmentation du marché intérieur pour ce qui est des schémas de certification dans l'Union.

(1 bis) Afin de garantir la résilience de l'Union face aux cyberattaques et de prévenir toute vulnérabilité sur le marché de l'Union, le présent règlement vise à compléter le cadre réglementaire horizontal établissant des exigences complètes en matière de cybersécurité pour tous les produits comportant des éléments numériques conformément au règlement (UE).../... du Parlement européen et du Conseil[5] (2022/0272 (COD)), en établissant des exigences essentielles pour les services de cybersécurité gérés, leur application et leur fiabilité.

(2) Les services de sécurité gérés, qui consistent à effectuer des activités liées à la gestion des risques en matière de cybersécurité de leurs clients, ou à fournir une assistance dans le cadre de ces activités, ***notamment en ce qui concerne la détection des incidents ainsi que la réponse apportée et le rétablissement à la suite de ceux-ci,*** ont gagné en importance en ce qui concerne la prévention et de la limitation des incidents de cybersécurité. ***Les activités des fournisseurs de services de sécurité gérés comprennent les services liés à la prévention, à l'identification, à la protection, à la détection, à l'analyse, à l'endiguement, à la réaction et au rétablissement, y compris, mais pas exclusivement, la fourniture de renseignements sur les cybermenaces, la surveillance des menaces en temps réel au moyen de techniques préventives, notamment la sécurité dès le stade de la conception, l'évaluation des risques, la détection élargie, la réparation et la***

---

4 Règlement (UE) 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) nº 526/2013 (règlement sur la cybersécurité) (JO L 151 du 7.6.2019, p. 15).

5 Règlement (UE) […/…] du Parlement européen et du Conseil du ... relatif à ... (JO L, …, ELI: …).

réaction. En conséquence, les fournisseurs de tels services sont considérés comme des entités essentielles ou importantes appartenant à un secteur hautement critique au titre de la directive (UE) 2022/2555 du Parlement européen et du Conseil[6]. Au titre du considérant 86 de ladite directive, les fournisseurs de services de sécurité gérés dans des domaines comme la réaction aux incidents, les tests d'intrusion, les audits de sécurité et le conseil jouent un rôle particulièrement important s'agissant de soutenir les efforts mis en œuvre par les entités pour prévenir et détecter les incidents, y réagir ou se rétablir après ceux-ci. Toutefois, des fournisseurs de services de sécurité gérés ont été eux-mêmes la cible de cyberattaques et, du fait de leur grande intégration dans les activités des opérateurs, ils représentent un risque particulier. Les entités essentielles et importantes au sens de la directive (UE) 2022/2555 doivent donc faire preuve d'une diligence renforcée lorsqu'elles sélectionnent leurs fournisseurs de services de sécurité gérés.

(3) Les fournisseurs de services de sécurité gérés jouent également un rôle important concernant la réserve de cybersécurité de l'UE, dont la mise en place progressive est soutenue par le règlement (UE).../… [établissant des mesures destinées à renforcer la solidarité et les capacités dans l'Union afin de détecter les menaces et incidents de cybersécurité, de s'y préparer et d'y réagir]. La réserve de cybersécurité de l'UE doit être utilisée pour soutenir les mesures de réaction et de rétablissement immédiat en cas d'incidents de cybersécurité importants et de grande ampleur. Le règlement (UE).../... [établissant des mesures destinées à renforcer la solidarité et les capacités dans l'Union afin de détecter les menaces et incidents de cybersécurité, de s'y préparer et d'y réagir] met en place un processus de sélection des fournisseurs constituant la réserve de cybersécurité de l'UE, qui devrait, entre autres, tenir compte du fait que le fournisseur concerné a obtenu une certification européenne ou nationale en matière de cybersécurité. Les services pertinents fournis par des fournisseurs de confiance au titre du règlement (UE).../... [établissant des mesures destinées à renforcer la solidarité et les capacités dans l'Union afin de détecter les

---

6 Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) nº 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (directive SRI 2) (JO L 333 du 27.12.2022, p. 80).

menaces et incidents de cybersécurité, de s'y préparer et d'y réagir] correspondent aux services de sécurité gérés conformément au présent règlement.

(4) La certification des services de sécurité gérés est non seulement pertinente dans le processus de sélection de la réserve de cybersécurité de l'UE, mais elle constitue également un indicateur de qualité essentiel pour les entités privées et publiques qui ont l'intention d'acheter de tels services. Compte tenu de la criticité des services de sécurité gérés et du caractère sensible des données qu'ils traitent, la certification pourrait fournir aux clients potentiels des orientations et une assurance importantes quant à la fiabilité de ces services. Les schémas européens de certification pour les services de sécurité gérés contribuent à éviter la fragmentation du marché unique. Le présent règlement vise donc à améliorer le fonctionnement du marché intérieur.

(4 bis) Les schémas européens de certification pour les services de sécurité gérés devraient conduire à l'adoption de ces services et à une concurrence accrue sur le terrain, en tenant compte des besoins spécifiques tant des fournisseurs que des bénéficiaires. Ces schémas devraient donc trouver un équilibre entre leur objectif et la charge réglementaire, administrative et financière potentielle que les fournisseurs, en particulier les microentreprises ou les petites et moyennes entreprises (PME), pourraient rencontrer. En outre, les schémas devraient encourager l'utilisation de services de sécurité gérés certifiés en contribuant à leur accessibilité, en particulier pour les petits acteurs, tels que les microentreprises et les PME, ainsi que pour les collectivités locales et régionales qui disposent de capacités et de ressources limitées, mais qui sont plus exposées aux atteintes à la cybersécurité ayant des implications financières, juridiques, de réputation et opérationnelles.

(4 ter) Le schéma de certification de l'Union pour les services de sécurité gérés devrait garantir la disponibilité de services sûrs et de haute qualité qui garantissent une transition numérique sûre et contribuent à la réalisation des objectifs fixés dans le programme d'action pour la décennie numérique, en particulier en ce qui concerne l'objectif consistant à ce que 75 % des entreprises de l'Union commencent à utiliser l'informatique en nuage, l'IA ou les mégadonnées, à ce que plus de 90 % des microentreprises et des PME atteignent au moins un niveau

élémentaire d'intensité numérique et à ce que les services publics essentiels soient proposés en ligne.

(4 quater) Dans le paysage numérique et technologique actuel, en évolution rapide, l'offre de ressources éducatives et de formations de nature formelle varie et les connaissances peuvent être acquises de différentes manières, tant formelles, par exemple au moyen de la fréquentation de l'université ou de cours, que non formelles, par exemple au moyen de formations professionnelles ou d'une expérience professionnelle de longue date dans le domaine concerné.

(5) Par rapport au déploiement de produits TIC, services TIC ou processus TIC, les services de sécurité gérés offrent en outre souvent des fonctionnalités de service supplémentaires qui dépendent des compétences, de l'expertise et de l'expérience de leur personnel. Afin de garantir la très grande qualité des services de sécurité gérés qui sont fournis, il convient de prévoir, dans le cadre des objectifs de sécurité, un très haut niveau de compétences, d'expertise et d'expérience ainsi que des procédures internes appropriées. Pour faire en sorte que tous les aspects d'un service de sécurité géré puissent être couverts par un schéma de certification ***spécifique***, il est par conséquent nécessaire de modifier le règlement (UE) 2019/881. L'***élaboration de schémas de certification établis en vertu du présent règlement devrait tenir compte des résultats et des recommandations de l'évaluation et de la révision prévues par le présent règlement.***

(5 bis) Afin de faciliter la croissance d'un marché de l'Union fiable, tout en créant des partenariats avec des pays tiers partageant les mêmes valeurs, notamment compte tenu des dispositions du règlement (UE).../... du Parlement européen et du Conseil[7] (2023/0109(COD)) en ce qui concerne l'accès à la réserve de cybersécurité de l'UE, le processus de certification établi dans le cadre fixé par le présent règlement devrait être rationalisé de manière à garantir la reconnaissance internationale et l'alignement sur les normes internationales.

(5 ter) Afin d'assurer le développement d'un marché de l'Union fiable pour les services de sécurité gérés, les fournisseurs de ces services et les États membres devraient

---

7 Règlement (UE) …/… du Parlement européen et du Conseil du ... relatif à ... (JO L, …, ELI: …).

collaborer et contribuer à la collecte de données sur la situation et l'évolution du marché du travail de la cybersécurité.

(5 quater) L'approche coordonnée à l'échelle de l'Union pour renforcer la résilience des infrastructures critiques repose sur le renforcement des capacités des États membres. Toutefois, l'Union est confrontée à une pénurie de talents, caractérisée par un manque de professionnels qualifiés et par l'évolution rapide des menaces, comme l'a reconnu la Commission dans sa communication du 18 avril 2023 sur l'Académie des compétences en matière de cybersécurité. Par conséquent, afin de faciliter l'émergence de services de sécurité gérés essentiels et de haute qualité et de disposer d'une meilleure vue d'ensemble de la composition de la main-d'œuvre de l'Union dans le domaine de la cybersécurité, il conviendrait de renforcer la coopération entre les États membres, la Commission, l'ENISA et les parties prenantes, y compris le secteur privé et le monde universitaire, par le développement de partenariats public-privé, le soutien aux initiatives de recherche et d'innovation, le développement et la reconnaissance mutuelle de normes communes et la certification des compétences en matière de cybersécurité, y compris par l'intermédiaire du cadre européen pour les compétences en matière de cybersécurité. Cela devrait également faciliter la mobilité des professionnels de la cybersécurité au sein de l'Union ainsi que l'intégration des connaissances et de la formation en matière de cybersécurité dans les programmes éducatifs, tout en garantissant l'accès aux apprentissages et aux stages pour les jeunes, y compris pour les personnes vivant dans des régions défavorisées, telles que les îles et les régions peu peuplées, rurales et isolées. Ces mesures devraient également viser à attirer davantage de femmes et de filles vers ce domaine et contribuer à combler l'écart entre les hommes et les femmes dans les domaines de la science, de la technologie, de l'ingénierie et des mathématiques. Le secteur privé devrait également s'efforcer de dispenser des formations sur le lieu de travail portant sur les compétences les plus recherchées, en associant l'administration publique et les jeunes entreprises, ainsi que les microentreprises et les PME.

(5 quinquies) Il convient de garantir un financement et des ressources appropriés aux fins des missions supplémentaires confiées à l'ENISA par les modifications qu'apporte au règlement (UE) 2019/881 le présent règlement.

(5 sexies) ***Afin de compléter certains éléments non essentiels du présent règlement, il convient de déléguer à la Commission le pouvoir d'adopter des actes conformément à l'article 290 du traité sur le fonctionnement de l'Union européenne afin de prévoir un schéma européen de certification de cybersécurité pour les produits TIC, services TIC, processus TIC et services de sécurité gérés. Il importe particulièrement que la Commission procède aux consultations appropriées durant son travail préparatoire, y compris au niveau des experts, et que ces consultations soient menées conformément aux principes définis dans l'accord interinstitutionnel du 13 avril 2016 «Mieux légiférer»[8] . En particulier, pour assurer leur égale participation à la préparation des actes délégués, le Parlement européen et le Conseil reçoivent tous les documents au même moment que les experts des États membres, et leurs experts ont systématiquement accès aux réunions des groupes d'experts de la Commission traitant de la préparation des actes délégués.***

(5 sexies) ***Le Contrôleur européen de la protection des données a été consulté conformément à l'article 42, paragraphe 1, du règlement (UE) 2018/1725 du Parlement européen et du Conseil et a rendu un avis le [JJ/MM/AAAA][9],***

ONT ADOPTÉ LE PRÉSENT RÈGLEMENT:

---

8 JO L 123 du 12.5.2016, p. 1.

9 JO C .../...

Article premier

Modifications du règlement (UE) 2019/881

Le règlement (UE) 2019/881 est modifié comme suit:

(1) À l'article 1er, paragraphe 1, premier alinéa, le point b) est remplacé par le texte suivant:

«b) un cadre pour la mise en place de schémas européens de certification de cybersécurité dans le but de garantir un niveau adéquat de cybersécurité des produits TIC, services TIC, processus TIC et services de sécurité gérés dans l'Union, ainsi que dans le but d'éviter la fragmentation du marché intérieur pour ce qui est des schémas de certification dans l'Union.»;

(2) L'article 2 est modifié comme suit:

a) les points 9), 10) et 11) sont remplacés par le texte suivant:

«9) "schéma européen de certification de cybersécurité", un ensemble complet de règles, d'exigences techniques, de normes et de procédures qui sont établies à l'échelon de l'Union et qui s'appliquent à la certification ou à l'évaluation de la conformité de produits TIC, services TIC, processus TIC ou services de sécurité gérés spécifiques;

10) "schéma national de certification de cybersécurité", un ensemble complet de règles, d'exigences techniques, de normes et de procédures élaborées et adoptées par une autorité publique nationale et qui s'appliquent à la certification ou à l'évaluation de la conformité des produits TIC, services TIC, processus TIC et services de sécurité gérés relevant de ce schéma spécifique;

11) "certificat de cybersécurité européen", un document délivré par un organisme compétent attestant qu'un produit TIC, service TIC, processus TIC ou service de sécurité géré donné a été évalué en ce qui concerne sa conformité aux exigences de sécurité spécifiques fixées dans un schéma européen de certification de cybersécurité;»;

b) le point suivant est inséré:

«14 bis) "service de sécurité géré", un service ***fourni à un tiers*** consistant

à effectuer des activités liées à la gestion des risques en matière de cybersécurité, ou à fournir une assistance ***ou des conseils*** dans le cadre de ces activités, y compris ***la réaction aux incidents***, les tests d'intrusion et les audits et missions de conseil en matière de sécurité»;

c) les points 20), 21) et 22) sont remplacés par le texte suivant:

«20) "spécification technique", un document qui établit les exigences techniques auxquelles un produit TIC, service TIC, processus TIC ou service de sécurité géré doit répondre ou des procédures d'évaluation de la conformité afférentes à un produit TIC, service TIC, processus TIC ou service de sécurité géré;

21) "niveau d'assurance", le fondement permettant de garantir qu'un produit TIC, service TIC, processus TIC ou service de sécurité géré satisfait aux exigences de sécurité d'un schéma européen de certification de cybersécurité spécifique, indique le niveau auquel un produit TIC, service TIC, processus TIC ou service de sécurité géré a été évalué mais, en tant que tel, ne mesure pas la sécurité du produit TIC, service TIC, processus TIC ou service de sécurité géré concerné;

22) "autoévaluation de la conformité", une action effectuée par un fabricant ou un fournisseur de produits TIC, services TIC, processus TIC ou services de sécurité gérés, qui évalue si ces produits TIC, services TIC, processus TIC ou services de sécurité gérés satisfont aux exigences fixées dans un schéma européen de certification de cybersécurité spécifique.»;

3) À l'article 4, le paragraphe 6 est remplacé par le texte suivant:

«6. L'ENISA favorise le recours à la certification européenne de cybersécurité en vue d'éviter la fragmentation du marché intérieur. L'ENISA contribue à l'établissement et au maintien d'un cadre européen de certification de cybersécurité, conformément au titre III du présent règlement, en vue de rendre plus transparente la cybersécurité des produits TIC, services TIC, processus TIC et services de sécurité gérés et, partant, de rehausser la confiance dans le marché intérieur numérique et la compétitivité de ce dernier.»;

4) L’article 8 est modifié comme suit:

a) le paragraphe 1 est remplacé par le texte suivant:

«1. L’ENISA soutient et favorise l’élaboration et la mise en œuvre de la politique de l’Union en matière de certification de cybersécurité des produits TIC, services TIC, processus TIC et services de sécurité gérés, telle qu’elle est établie au titre III du présent règlement:

a) en surveillant, en permanence, les évolutions dans les domaines connexes de la normalisation et en recommandant des spécifications techniques d’utilisation appropriées dans le développement des schémas européens de certification de cybersécurité en application de l’article 54, paragraphe 1, point c), dans les cas où il n’existe aucune norme;

b) en préparant des schémas européens de certification de cybersécurité candidats (ci-après dénommés “schémas candidats”) pour des produits TIC, services TIC, processus TIC et services de sécurité gérés, conformément à l’article 49;

c) en évaluant les schémas européens de certification de cybersécurité, conformément à l’article 49, paragraphe 8;

d) en participant aux examens par les pairs, conformément à l’article 59, paragraphe 4;

e) en aidant la Commission à assurer le secrétariat du GECC, conformément à l’article 62, paragraphe 5.»;

b) le paragraphe 3 est remplacé par le texte suivant:

«3. L’ENISA compile et publie des lignes directrices et met au point des bonnes pratiques en ce qui concerne les exigences de cybersécurité de produits TIC, services TIC, processus TIC et services de sécurité gérés, en coopération avec les autorités nationales de certification de cybersécurité et les entreprises du secteur d’une façon formelle, structurée et transparente.»;

c) le paragraphe 5 est remplacé par le texte suivant:

«5. L'ENISA facilite l'établissement et l'adoption de normes européennes et internationales en matière de gestion des risques et de sécurité des produits TIC, services TIC, processus TIC et services de sécurité gérés.»;

5) À l'article 46, les paragraphes 1 et 2 sont remplacés par le texte suivant:

«1. Le cadre européen de certification de cybersécurité est établi afin d'améliorer les conditions de fonctionnement du marché intérieur en renforçant le niveau de cybersécurité au sein de l'Union et en permettant de disposer, au niveau de l'Union, d'une approche harmonisée en ce qui concerne les schémas européens de certification de cybersécurité, en vue de créer un marché unique numérique pour les produits TIC, services TIC, processus TIC et services de sécurité gérés.

2. Le cadre européen de certification de cybersécurité prévoit un mécanisme visant à établir des schémas européens de certification de cybersécurité. Il atteste que les produits TIC, services TIC et processus TIC qui ont été évalués conformément à ces schémas satisfont à des exigences de sécurité définies, dans le but de protéger la disponibilité, l'authenticité, l'intégrité ou la confidentialité des données stockées, transmises ou traitées ou des fonctions ou services qui sont offerts par ces produits, services et processus ou accessibles par leur intermédiaire tout au long de leur cycle de vie. En outre, il atteste que les services de sécurité gérés qui ont été évalués conformément à ces schémas satisfont à des exigences de sécurité définies, dans le but de protéger la disponibilité, l'authenticité, l'intégrité et la confidentialité des données qui sont consultées, traitées, stockées ou transmises dans le cadre de la fourniture de ces services, et que ces services sont fournis en permanence avec la compétence, l'expertise et l'expérience requises par un personnel possédant un très haut niveau de connaissances techniques pertinentes et d'intégrité professionnelle.»;

6) À l'article 47, les paragraphes 2 et 3 sont remplacés par le texte suivant:

«2. Le programme de travail glissant de l'Union inclut notamment une liste de produits TIC, services TIC et processus TIC ou de catégories de ceux-ci, ainsi que de services de sécurité gérés, qui sont susceptibles de bénéficier d'une inclusion dans le champ d'application d'un schéma européen de certification de

cybersécurité. ***Dans ce contexte, la Commission peut inclure une évaluation approfondie des parcours de formation existants, afin de combler les déficits de compétences recensés, et une liste de propositions visant à répondre aux besoins en personnel qualifié et en types de compétences.***

3. L'inclusion de produits TIC, services TIC et processus TIC spécifiques ou de catégories spécifiques de ceux-ci, ou de services de sécurité gérés, dans le programme de travail glissant de l'Union doit se justifier sur la base de l'un ou de plusieurs des motifs suivants:

a) la disponibilité et le développement de schémas nationaux de certification de cybersécurité couvrant toute catégorie spécifique de produits TIC, services TIC, processus TIC ou services de sécurité gérés et, en particulier, en ce qui concerne le risque de fragmentation;

b) le droit ou la politique applicable de l'Union ou d'un État membre;

c) la demande du marché;

c bis) les évolutions technologiques ainsi que la disponibilité et le développement de systèmes internationaux de certification de cybersécurité et de normes internationales et industrielles.

d) l'évolution de la situation en ce qui concerne les cybermenaces;

e) une demande de préparation d'un schéma candidat spécifique par le GECC.»;

7) L'article 49 ***est modifié comme suit***:

a) le paragraphe 7 est remplacé par le texte suivant:

«7. La Commission, se fondant sur le schéma candidat préparé par l'ENISA, ***est habilitée à*** adopter des actes ***délégués conformément à l'article 65 bis, qui complètent le présent règlement en*** prévoyant un schéma européen de certification de cybersécurité pour les produits TIC, services TIC, processus TIC et services de sécurité gérés qui satisfont aux exigences des articles 51, 52 et 54.***»;***

b) Le paragraphe suivant est inséré:

«7 bis. Avant d'adopter de tels actes délégués, la Commission, en coopération avec l'ENISA, réalise et publie une analyse d'impact de la proposition de schéma européen de certification de cybersécurité. Lors de la préparation de cette analyse d'impact, la Commission procède à des consultations publiques et consulte le groupe de certification de la cybersécurité des parties prenantes et le groupe européen de certification de cybersécurité.»;

8) L'article 51 est modifié comme suit:

a) le titre est remplacé par le texte suivant:

«Objectifs de sécurité des schémas européens de certification de cybersécurité pour les produits TIC, services TIC et processus TIC»

b) la phrase introductive est remplacée par le texte suivant:

«Un schéma européen de certification de cybersécurité pour les produits TIC, services TIC ou processus TIC est conçu de façon à réaliser, selon le cas, au moins les objectifs de sécurité suivants:»***;***

9) L'article suivant est inséré:

«Article 51 bis Objectifs de sécurité des schémas européens de certification de cybersécurité pour les services de sécurité gérés

Un schéma européen de certification de cybersécurité pour les services de sécurité gérés est conçu de façon à réaliser, selon le cas, au moins les objectifs de sécurité suivants:

a) faire en sorte que les services de sécurité gérés soient fournis avec la compétence, l'expertise et l'expérience requises, y compris que le personnel chargé de fournir ces services possède un très haut niveau de compétence et de connaissances techniques dans le domaine spécifique, une expérience suffisante et appropriée et la plus haute intégrité professionnelle;

b) faire en sorte que le fournisseur ait mis en place des procédures internes appropriées pour garantir que les services de sécurité gérés sont fournis à tout moment à un niveau de qualité très élevé;

c) protéger les données consultées, stockées, transmises ou traitées de toute autre façon dans le cadre de la fourniture de services de sécurité gérés contre l'accès, le stockage, la diffusion, la destruction ou tout autre traitement accidentels ou non autorisés, ou contre la perte ou l'altération ou l'indisponibilité;

d) faire en sorte que la disponibilité des données, services et fonctions ainsi que l'accès à ceux-ci soient rétablis dans les plus brefs délais en cas d'incident physique ou technique;

e) faire en sorte que les personnes autorisées, les programmes ou les machines ne puissent accéder qu'aux données, services ou fonctions concernés par leurs droits d'accès;

f) garder une trace des données, services ou fonctions qui ont été consultés, utilisés ou traités de toute autre façon, du moment où ils l'ont été et par qui, et faire en sorte qu'il soit possible d'évaluer ces éléments;

g) faire en sorte que les produits TIC, services TIC et processus TIC déployés dans le cadre de la fourniture des services de sécurité gérés soient sécurisés par défaut et dès la conception, ***et soient dotés de logiciels et d'équipements à jour,*** ne contiennent pas de vulnérabilités connues et comprennent les dernières mises à jour de sécurité;

10) L'article 52 est modifié comme suit:

a) le paragraphe 1 est remplacé par le texte suivant:

«1. Un schéma européen de certification de cybersécurité peut préciser un ou plusieurs des niveaux d'assurance suivants pour les produits TIC, services TIC, processus TIC et services de sécurité gérés: "élémentaire", "substantiel" ou "élevé". Le niveau d'assurance correspond au niveau de risque associé à l'utilisation prévue du produit TIC, service TIC, processus TIC ou service de sécurité géré, en termes de probabilité et de répercussions d'un incident.»;

b) le paragraphe 3 est remplacé par le texte suivant:

«3. Les exigences de sécurité correspondant à chaque niveau d'assurance sont fournies dans le schéma européen de certification de cybersécurité

concerné, y compris les fonctionnalités de sécurité correspondantes ainsi que la rigueur et l'ampleur correspondantes de l'évaluation à laquelle le produit TIC, service TIC, processus TIC ou service de sécurité géré doit être soumis.»;

c) les paragraphes 5, 6 et 7 sont remplacés par le texte suivant:

«5. Un certificat de cybersécurité européen ou une déclaration de conformité de l'Union européenne qui se réfère au niveau d'assurance dit "élémentaire" offre l'assurance que les produits TIC, services TIC, processus TIC et services de sécurité gérés pour lesquels ce certificat ou cette déclaration de conformité de l'Union européenne est délivré(e) satisfont aux exigences de sécurité correspondantes, y compris les fonctionnalités de sécurité, et qu'ils ont été évalués à un niveau qui vise à minimiser les risques élémentaires connus d'incidents et de cyberattaques. Les activités d'évaluation à entreprendre comprennent au moins un examen de la documentation technique. Lorsqu'un tel examen n'est pas approprié, des activités d'évaluation de substitution ayant un effet équivalent sont entreprises.

6. Un certificat de cybersécurité européen qui se réfère au niveau d'assurance dit "substantiel" offre l'assurance que les produits TIC, services TIC, processus TIC et services de sécurité gérés pour lesquels ce certificat est délivré satisfont aux exigences de sécurité correspondantes, y compris des fonctionnalités de sécurité, et qu'ils ont été évalués à un niveau qui vise à minimiser les risques liés à la cybersécurité connus, et le risque d'incidents et de cyberattaques émanant d'acteurs aux aptitudes et aux ressources limitées. Les activités d'évaluation à entreprendre comprennent au moins: un examen visant à démontrer l'absence de vulnérabilités connues du public et des vérifications tendant à démontrer que les produits TIC, services TIC, processus TIC ou services de sécurité gérés mettent correctement en œuvre les fonctionnalités de sécurité nécessaires. Lorsque de telles activités d'évaluation ne sont pas appropriées, des activités d'évaluation de substitution ayant un effet équivalent sont entreprises.

7. Un certificat de cybersécurité européen qui se réfère au niveau d'assurance dit "élevé" offre l'assurance que les produits TIC, services TIC, processus TIC et services de sécurité gérés pour lesquels ce certificat est délivré satisfont aux exigences de sécurité correspondantes, y compris des fonctionnalités de sécurité, et qu'ils ont été évalués à un niveau qui vise à minimiser le risque que des cyberattaques de pointe soient menées par des acteurs aux aptitudes solides et aux ressources importantes. Les activités d'évaluation à entreprendre comprennent au moins: un examen démontrant l'absence de vulnérabilités connues du public, des vérifications tendant à démontrer que les produits TIC, services TIC, processus TIC ou services de sécurité gérés mettent correctement en œuvre les fonctionnalités de sécurité nécessaires, au niveau de l'état de l'art et une évaluation de leur résistance à des attaques menées par des acteurs compétents, au moyen de tests d'intrusion. Lorsque de telles activités d'évaluation ne sont pas appropriées, des activités d'évaluation de substitution ayant un effet équivalent sont entreprises.»;

(11) À l'article 53, les paragraphes 1, 2 et 3 sont remplacés par le texte suivant:

«1. Un schéma européen de certification de cybersécurité peut permettre la réalisation d'une autoévaluation de la conformité sous la seule responsabilité du fabricant ou du fournisseur de produits TIC, services TIC, processus TIC ou services de sécurité gérés. L'autoévaluation de la conformité n'est autorisée que pour les produits TIC, services TIC, processus TIC et services de sécurité gérés qui présentent un risque faible correspondant au niveau d'assurance dit "élémentaire".

2. Le fabricant ou le fournisseur de produits TIC, services TIC, processus TIC ou services de sécurité gérés peut délivrer une déclaration de conformité de l'Union européenne indiquant que le respect des exigences énoncées dans le schéma a été démontré. En délivrant une telle déclaration, le fabricant ou fournisseur de produits TIC, services TIC, processus TIC ou services de sécurité gérés assume la responsabilité du respect par le produit TIC, service TIC, processus TIC ou service de sécurité géré des exigences fixées dans ce

schéma.

3. Le fabricant ou fournisseur de produits TIC, services TIC, processus TIC ou services de sécurité gérés garde à la disposition de l'autorité nationale de certification de cybersécurité visée à l'article 58 la déclaration de conformité de l'Union européenne, la documentation technique et toutes les autres informations pertinentes relatives à la conformité des produits TIC, services TIC, processus TIC ou services de sécurité gérés avec le schéma pendant la durée prévue dans le schéma européen de certification de cybersécurité correspondant. Une copie de la déclaration de conformité de l'Union européenne est transmise à l'autorité nationale de certification de cybersécurité et à l'ENISA.»;

(12) À l'article 54, le paragraphe 1 est modifié comme suit:

a) le point a) est remplacé par le texte suivant:

«a) l'objet et le champ d'application du schéma de certification, notamment le type ou les catégories de produits TIC, services TIC, processus TIC et services de sécurité gérés couverts;»;

b) le point j) est remplacé par le texte suivant:

«j) les règles relatives au contrôle du respect par les produits TIC, services TIC, processus TIC et services de sécurité gérés des exigences liées aux certificats de cybersécurité européens ou aux déclarations de conformité de l'Union européenne, notamment les mécanismes permettant de démontrer le respect constant des exigences de cybersécurité qui ont été définies;»;

c) le point l) est remplacé par le texte suivant:

«l) les règles relatives aux conséquences pour les produits TIC, services TIC, processus TIC et services de sécurité gérés qui ont été certifiés ou pour lesquels une déclaration de conformité de l'Union européenne a été délivrée, mais qui ne respectent pas les exigences du schéma;»;

d) le point o) est remplacé par le texte suivant:

«o) l'identification des schémas nationaux ou internationaux de certification

de cybersécurité couvrant le même type ou les mêmes catégories de produits TIC, services TIC, processus TIC et services de sécurité gérés, d'exigences de sécurité, de critères et méthodes d'évaluation et de niveaux d'assurance;»;

e) le point q) est remplacé par le texte suivant:

«q) la période de disponibilité de la déclaration de conformité de l'Union européenne, de la documentation technique et de toutes les autres informations pertinentes qui doivent être mises à disposition par le fabricant ou le fournisseur de produits TIC, services TIC, processus TIC ou services de sécurité gérés;»;

(13) L'article 56 est modifié comme suit:

a) le paragraphe 1 est remplacé par le texte suivant:

«1. Les produits TIC, services TIC, processus TIC et services de sécurité gérés qui ont été certifiés dans le cadre d'un schéma européen de certification de cybersécurité adopté en vertu de l'article 49 sont présumés respecter les exigences de ce schéma.»;

b) le paragraphe 3 est modifié comme suit:

i) le premier alinéa est remplacé par le texte suivant:

«La Commission évalue régulièrement l'efficacité et l'utilisation des schémas européens de certification de cybersécurité adoptés ainsi que la question de savoir si un schéma européen de certification de cybersécurité spécifique doit être rendu obligatoire, au moyen de dispositions pertinentes du droit de l'Union, pour garantir un niveau adéquat de cybersécurité des produits TIC, services TIC, processus TIC et services de sécurité gérés dans l'Union, et améliorer le fonctionnement du marché intérieur. La première de ces évaluations est effectuée le 31 décembre 2023 au plus tard, et les évaluations suivantes sont effectuées au moins tous les deux ans par la suite. Sur la base des résultats de ces évaluations, la Commission recense les produits TIC, services TIC, processus TIC services de sécurité gérés couverts par un schéma de

certification existant qui doivent relever d'un schéma de certification obligatoire.»;

ii) le troisième alinéa est modifié comme suit:

a bis) le point a) est remplacé par le texte suivant:

«a) tient compte de l'incidence des mesures, du point de vue des coûts, sur les fabricants ou fournisseurs de ces produits TIC, services TIC, processus TIC ou services de sécurité gérés et sur les utilisateurs, ainsi que des avantages sociétaux ou économiques résultant du renforcement escompté du niveau de sécurité des produits TIC, services TIC, processus TIC ou services de sécurité gérés ciblés;

b ter) le point d) est remplacé par le texte suivant:

«d) prend en considération les délais de mise en œuvre ainsi que les mesures et périodes transitoires, en ce qui concerne, en particulier, l'incidence éventuelle de la mesure sur les fabricants ou les fournisseurs de produits TIC, services TIC, processus TIC ou services de sécurité gérés, y compris ***les intérêts et les besoins spécifiques des microentreprises et des PME***;»***;***

iii) l'alinéa suivant est ajouté:

«En ce qui concerne le troisième alinéa, point d), du présent article, la Commission assure un soutien financier approprié dans le cadre réglementaire des programmes existants de l'Union, notamment afin d'alléger la charge financière pesant sur les microentreprises et les PME, y compris les jeunes pousses actives dans le domaine des services de sécurité gérés.»;

c) les paragraphes 7 et 8 sont remplacés par le texte suivant:

«7. La personne physique ou morale qui soumet des produits TIC, services TIC, processus TIC ou services de sécurité gérés à la certification met à la disposition de l'autorité nationale de certification de cybersécurité

visée à l'article 58, lorsque cette autorité est l'organisme délivrant le certificat de cybersécurité européen, ou de l'organisme d'évaluation de la conformité visé à l'article 60 toutes les informations nécessaires pour procéder à la certification.

8. Le titulaire d'un certificat de cybersécurité européen informe l'autorité ou l'organisme visé au paragraphe 7 de toute vulnérabilité ou irrégularité détectée ultérieurement concernant la sécurité du produit TIC, service TIC, processus TIC ou service de sécurité géré certifié susceptible d'avoir une incidence sur son respect des exigences liées à la certification. Cette autorité ou cet organisme transmet ces informations sans retard injustifié à l'autorité nationale de certification de cybersécurité concernée.»

(14) À l'article 57, les paragraphes 1 et 2 sont remplacés par le texte suivant:

«1. Sans préjudice du paragraphe 3 du présent article, les schémas nationaux de certification de cybersécurité et les procédures connexes pour les produits TIC, services TIC, processus TIC et services de sécurité gérés couverts par un schéma européen de certification de cybersécurité cessent de produire leurs effets à partir de la date fixée dans l'acte ***délégué*** adopté en application de l'article 49, paragraphe 7. Les schémas nationaux de certification de cybersécurité et les procédures connexes pour les produits TIC, services TIC, processus TIC et services de sécurité gérés qui ne sont pas couverts par un schéma européen de certification de cybersécurité continuent à exister.

2. Les États membres s'abstiennent d'instaurer de nouveaux schémas nationaux de certification de cybersécurité pour les produits TIC, services TIC, processus TIC et services de sécurité gérés qui sont déjà couverts par un schéma européen de certification de cybersécurité en vigueur.»;

(15) L'article 58 est modifié comme suit:

(a) le paragraphe 7 est modifié comme suit:

(i) les points a) et b) sont remplacés par le texte suivant:

«a) supervisent et font respecter les règles prévues dans les schémas

européens de certification de cybersécurité, en application de l'article 54, paragraphe 1, point j), aux fins du contrôle du respect par les produits TIC, services TIC, processus TIC et services de sécurité gérés des exigences des certificats de cybersécurité européens délivrés sur leurs territoires respectifs, en coopération avec les autres autorités compétentes de surveillance du marché;

b) contrôlent le respect des obligations qui incombent aux fabricants ou fournisseurs de produits TIC, services TIC, processus TIC ou services de sécurité gérés qui sont établis sur leurs territoires respectifs et qui procèdent à une autoévaluation de conformité et font respecter ces obligations, et contrôlent, en particulier, le respect des obligations de ces fabricants ou fournisseurs visées à l'article 53, paragraphes 2 et 3, et dans le schéma européen de certification de cybersécurité correspondant, et font respecter ces obligations;»;

(ii) le point h) est remplacé par le texte suivant:

«(h) coopèrent avec les autres autorités nationales de certification de cybersécurité ou d'autres autorités publiques, notamment en partageant des informations sur l'éventuel non-respect par des produits TIC, services TIC, processus TIC et services de sécurité gérés des exigences du présent règlement ou des exigences de schémas de certification de cybersécurité spécifiques; et»;

(b) le paragraphe 9 est remplacé par le texte suivant:

«9. Les autorités nationales de certification de cybersécurité coopèrent entre elles et avec la Commission et échangent notamment des informations, expériences et bonnes pratiques en ce qui concerne la certification de cybersécurité et les questions techniques relatives à la cybersécurité des produits TIC, services TIC, processus TIC et services de sécurité gérés.»;

(16) À l'article 59, paragraphe 3, les points b) et c) sont remplacés par le texte suivant:

«b) les procédures permettant de superviser et de faire respecter les règles relatives au contrôle du respect par les produits TIC, services TIC, processus TIC et

services de sécurité gérés des certificats de cybersécurité européens, conformément à l'article 58, paragraphe 7, point a);

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

(16 bis) L'article suivant est inséré:

Article 65 bis
Exercice de la délégation

1. Le pouvoir d'adopter des actes délégués conféré à la Commission est soumis aux conditions fixées au présent article.

2. Le pouvoir d'adopter des actes délégués visé à l'article 49, paragraphe 7, est conféré à la Commission pour une période de cinq ans à compter du ... [date d'entrée en vigueur du règlement modifié]. La Commission élabore un rapport relatif à la délégation de pouvoir au plus tard neuf mois avant la fin de la période de cinq ans. La délégation de pouvoir est tacitement prorogée pour des périodes d'une durée identique, sauf si le Parlement européen ou le Conseil s'oppose à cette prorogation trois mois au plus tard avant la fin de chaque période.

3. La délégation de pouvoir visée à l'article 7 peut être révoquée à tout moment par le Parlement européen ou le Conseil. La décision de révocation met fin à la délégation de pouvoir qui y est précisée. La révocation prend effet le jour suivant celui de la publication de ladite décision au Journal officiel de l'Union européenne ou à une date ultérieure qui est précisée dans ladite décision. Elle ne porte pas atteinte à la validité des actes délégués déjà en vigueur.

4. Avant l'adoption d'un acte délégué, la Commission consulte les experts désignés par chaque État membre, conformément aux principes définis dans l'accord interinstitutionnel du 13 avril 2016 «Mieux légiférer».

5. Aussitôt qu'elle adopte un acte délégué, la Commission le notifie au Parlement européen et au Conseil simultanément.

6. Un acte délégué adopté en vertu de l'article 49, paragraphe 7, n'entre en vigueur que si le Parlement européen ou le Conseil n'a pas exprimé d'objections dans un délai de deux mois à compter de la notification de cet acte au Parlement européen et au Conseil ou si, avant l'expiration de ce délai, le Parlement européen et le Conseil ont tous deux informé la Commission de leur intention de ne pas exprimer d'objections. Ce délai est prolongé de deux mois à l'initiative du Parlement européen ou du Conseil.;»

(17) L'article 67 est remplacé par le texte suivant:

«Article 67

Évaluation et révision

1. Au plus tard le 28 juin 2024, et tous les trois ans par la suite, la Commission évalue l'incidence, l'efficacité et l'efficience de l'ENISA et de ses méthodes de travail, ainsi que la nécessité éventuelle de modifier le mandat de l'ENISA et les conséquences financières d'une telle modification. L'évaluation tient compte de toute information communiquée en retour à l'ENISA en réaction à ses activités. Lorsque la Commission estime que le maintien du fonctionnement de l'ENISA n'est plus justifié au regard des objectifs, du mandat et des tâches qui lui ont été assignées, elle peut proposer que les dispositions du présent règlement relatives à l'ENISA soient modifiées.

2. L'évaluation porte sur les effets, l'efficacité et l'efficience des dispositions du titre III du présent règlement au regard des objectifs consistant à garantir un niveau adéquat de cybersécurité des produits TIC, services TIC, processus TIC et services de sécurité gérés dans l'Union et à améliorer le fonctionnement du marché intérieur.

3. L'évaluation porte également sur:

a) l'efficience et l'efficacité des procédures conduisant à la consultation, à la préparation et à l'adoption des systèmes européens de certification en matière de cybersécurité, ainsi que les moyens d'améliorer et d'accélérer ces procédures;

b) la nécessité ou non de fixer des exigences essentielles en matière de

cybersécurité comme condition d'accès au marché intérieur pour empêcher que des produits TIC, services TIC, processus TIC et services de sécurité gérés qui ne satisfont pas aux exigences de base en matière de cybersécurité entrent sur le marché de l'Union.

4. Au plus tard le 28 juin 2024, et tous les trois ans par la suite, la Commission transmet le rapport d'évaluation, accompagné de ses conclusions, au Parlement européen, au Conseil et au conseil d'administration. Les conclusions de ce rapport sont rendues publiques.»

Article 2

Le présent règlement entre en vigueur le vingtième jour suivant celui de sa publication au Journal officiel de l'Union européenne.

Le présent règlement est obligatoire dans tous ses éléments et directement applicable dans tout État membre.

Fait à ...,

Par le Parlement européen	*Par le Conseil*
La présidente	*Le président*

EXPOSÉ DES MOTIFS

La rapporteure soutient la proposition de règlement du Parlement européen et du Conseil modifiant le règlement (UE) 2019/881 en ce qui concerne les services de sécurité gérés et comprend la nécessité de mettre à jour et de renforcer le schéma européen de certification de cybersécurité en faisant en sorte qu'il couvre des services industriels importants et en pleine croissance. Certains États membres ayant déjà commencé à adopter des schémas de certification pour les services de sécurité gérés, la rapporteure estime que cette modification du règlement sur la cybersécurité est essentielle pour éviter des divergences importantes entre les schémas nationaux, lesquelles entraîneraient une forme de fragmentation du marché allant à l'encontre des intérêts économiques et stratégiques de l'Union.

À cet égard, il est reconnu que la présente proposition vise à compléter le règlement sur la cybersolidarité; cette extension spécifique du schéma européen de certification de cybersécurité permettra en particulier aux services de sécurité gérés – correspondant aux «fournisseurs de confiance» du règlement sur la cybersolidarité – de jouer un rôle important dans la future réserve de cybersécurité de l'UE. Par conséquent, la présente proposition revêt également une grande importance pour favoriser l'élargissement des capacités de l'Union en matière de cybersécurité, essentiel pour contrer les menaces potentielles dans une situation géopolitique en constante évolution.

Dans les limites de la proposition de la Commission, l'objectif de la rapporteure est de consolider cette modification ciblée du règlement sur la cybersécurité et de lui apporter davantage de clarté. Cet objectif apparaît dans les modifications apportées par la rapporteure à la définition des services de sécurité gérés, qui précise qu'ils sont «externalisés», tout en détaillant davantage ce que peut recouvrir la définition. Les amendements déposés concernant la reconnaissance des normes internationales en matière de cybersécurité visent à renforcer la confiance tout en mettant au point des règles globales au niveau de l'Union.

Le présent projet de rapport met davantage l'accent sur la lutte contre le déficit de compétences et sur le soutien aux micro, petites et moyennes entreprises. En ce qui concerne

le premier point, les amendements déposés se fondent sur la nécessité déjà implicite des compétences dans le cadre du système de certification de cybersécurité eu égard à «la compétence, l'expertise et l'expérience requises par un personnel possédant un très haut niveau de connaissances techniques pertinentes et d'intégrité professionnelle». De l'avis de la rapporteure, le schéma européen de certification doit non seulement favoriser la coopération entre tous les acteurs concernés ainsi qu'entre les États membres, le secteur privé, le monde universitaire et les instituts de recherche, mais aussi encourager l'élaboration d'une nouvelle feuille de route pour la formation et l'autonomisation de la main-d'œuvre, en collectant davantage de données sur les compétences nécessaires et en contribuant à combler l'écart entre les hommes et les femmes dans les STIM.

Dans le même temps, les micro, petites et moyennes entreprises, qui constituent l'épine dorsale de l'économie européenne et ont assurément un rôle positif à jouer dans le secteur de la cybersécurité, devraient bénéficier d'un soutien financier suffisant dans le cadre réglementaire des programmes existants de l'Union afin d'alléger toute charge financière disproportionnée qui pèserait sur elles.

21.9.2023

LETTRE DE LA COMMISSION DU MARCHÉ INTÉRIEUR ET DE LA PROTECTION DES CONSOMMATEURS

M. Cristian Silviu Buşoi
Président
Commission de l'industrie, de la recherche et de l'énergie
BRUXELLES

Objet: Avis sur la proposition de règlement du Parlement européen et du Conseil modifiant le règlement (UE) 2019/881 en ce qui concerne les services de sécurité gérés (COM(2023)0208 – C9-0137/2023 – 2023/0108(COD))

Monsieur le Président,

Dans le cadre de la procédure en objet, la commission du marché intérieur et de la protection des consommateurs a été chargée de soumettre un avis à votre commission. Au cours de sa réunion du 23 mai 2023, elle a décidé de transmettre cet avis sous forme de lettre. Elle a examiné la question et adopté l'avis lors de sa réunion du 19 septembre 2023.

Lors de cette réunion[1], elle a décidé d'inviter la commission de l'industrie, de la recherche et de l'énergie (ITRE), compétente au fond, à incorporer dans le rapport législatif qu'elle adoptera les suggestions suivantes.

Je vous prie d'agréer, Monsieur le Président, l'expression de ma haute considération.

Anna Cavazzini

SUGGESTIONS

La commission du marché intérieur et de la protection des consommateurs invite la commission de l'industrie, de la recherche et de l'énergie, compétente au fond, à prendre en considération les suggestions suivantes:

A. considérant que la Commission a publié, le 18 avril 2023, une proposition législative sur les services de sécurité gérés qui comporte des modifications ciblées du règlement de

[1] Étaient présents au moment du vote final: Anna Cavazzini (présidente), Andrus Ansip (vice-président), Krzysztof Hetman (vice-président), Alex Agius Saliba, João Albuquerque, Pablo Arias Echeverría, Laura Ballarín Cereza, Alessandra Basso, Brando Benifei, Biljana Borzan, Vlad Marius Botoş, Deirdre Clune, Dita Charanzová, David Cormand, Carlo Fidanza, Malte Gallée, Sandro Gozi, Svenja Hahn, Virginie Joron, Eugen Jurzyca, Arba Kokalari, Marcel Kolaja, Andrey Kovatchev, Jean-Lin Lacapelle, Morten Løkkegaard, Beata Mazurek, Leszek Miller, Anne Sophie Pelletier, Christel Schaldemose, Andreas Schwab, Tomislav Sokol, Ivan Štefanec, Róża Thun und Hohenstein, Tom Vandenkendelaere, Kim Van Sparrentak.

l'Union sur la cybersécurité[2];

B. considérant que, sur la proposition législative relative au règlement de l'Union sur la cybersécurité (2017/0225(COD))[3], la commission du marché intérieur et de la protection des consommateurs (IMCO) a soumis, au titre de l'ancien article 54 du règlement intérieur, un avis à la commission de l'industrie, de la recherche et de l'énergie (ITRE) compétente au fond, avec des compétences partagées en ce qui concerne le cadre de certification de cybersécurité, étant donné la compétence claire de la commission IMCO en ce qui concerne les systèmes de certification et, en général, la normalisation, la surveillance du marché et la mise en œuvre du marché unique numérique;

C. considérant que le règlement de l'Union sur la cybersécurité[4] vise à atteindre 1) un niveau élevé de cybersécurité, de cyberrésilience et de confiance dans l'Union en déterminant les objectifs, les missions et les questions organisationnelles pour une agence renforcée et rebaptisée «Agence de l'Union européenne pour la cybersécurité» (ENISA), dotée d'un nouveau mandat permanent, et 2) un cadre pour des schémas européens de certification de cybersécurité pour les produits, services et processus des technologies de l'information et de la communication (TIC);

D. considérant les modifications ciblées proposées pour inclure les services de sécurité gérés dans le champ d'application du règlement de l'Union sur la cybersécurité et y ajouter une définition de ces services qui est étroitement alignée sur la définition figurant dans la directive SRI 2[5]; considérant que ces modifications permettraient à la Commission, au moyen d'actes d'exécution, d'adopter des schémas européens de certification de cybersécurité pour les services de sécurité gérés, en plus des produits, services et processus TIC, déjà couverts par le règlement de l'Union sur la cybersécurité;

E. considérant que les services de sécurité gérés jouent un rôle de plus en plus important dans la prévention et la limitation des incidents de cybersécurité;

1. constate que, le 23 mai 2022[6], le Conseil a appelé à une augmentation du niveau global de cybersécurité dans l'Union en facilitant l'émergence et le développement de fournisseurs de services de cybersécurité fiables; estime notamment que la guerre en Ukraine, le contexte géopolitique actuel et les menaces continues des régimes de pays tiers, ainsi que la croissance constante du marché des technologies numériques et la transformation numérique des processus en général ont entraîné le besoin d'un niveau plus élevé de cybersécurité dans l'Union et ses États membres; recommande à la Commission de prendre des mesures volontaristes pour soutenir le développement de fournisseurs de services de cybersécurité fiables, telles que le financement de la recherche et du développement, des programmes de formation visant à renforcer les compétences en matière de cybersécurité et des incitations pour les entreprises à investir dans la cybersécurité; propose que l'Union renforce sa coopération avec l'OTAN et d'autres partenaires internationaux afin de répondre aux cybermenaces émanant des régimes de pays tiers, y compris en partageant des renseignements sur les menaces, en menant des

[2] https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:52023PC0208
[3] https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?lang=fr&reference=2017/0225(OLP)
[4] JO L 151 du 7.6.2019, p. 15
[5] JO L 333/810 du 27.12.2022
[6] 9364/22

exercices conjoints et en apportant des réponses coordonnées aux cyberattaques;

2. souligne que la certification des services de sécurité gérés, fondée sur des règles non discriminatoires et reflétant les normes européennes et internationales, est essentielle pour instaurer et garantir la confiance dans la qualité de ces services, notamment dans le but d'atteindre un niveau élevé de protection des consommateurs; constate que certains États membres ont d'ores et déjà adopté des systèmes de certification pour les services de sécurité gérés et qu'il est donc essentiel d'éviter la fragmentation du marché intérieur et les incohérences, qui peuvent affecter le secteur et les entreprises de la cybersécurité, ainsi que de permettre une approche harmonisée par la création, pour ces services, d'un schéma européen de certification de cybersécurité; demande que le cadre de certification de cybersécurité intègre les bonnes pratiques des systèmes nationaux de certification existants et soit élaboré en consultation avec les principaux acteurs du secteur de la cybersécurité;

3. souligne que les prestataires de services de sécurité gérés dans des domaines comme la réaction aux incidents, les tests d'intrusion, les audits de sécurité et les services de conseil jouent un rôle important s'agissant de soutenir les entités dans leurs efforts pour prévenir et détecter les cyberincidents, y réagir ou se rétablir après ceux-ci; estime qu'étant donné que de plus en plus d'entreprises peinent à entretenir divers systèmes logiciels complexes et réseaux d'entreprise interconnectés, elles dépendent nécessairement de fournisseurs de services de sécurité gérés et que, par conséquent, ces fournisseurs devraient être considérés comme un élément essentiel de l'écosystème de la cybersécurité de l'Union; note toutefois que les fournisseurs de services de sécurité gérés ont été eux-mêmes la cible de cyberattaques et que, du fait de leur grande intégration dans les activités des opérateurs, ils peuvent présenter un risque particulier;

4. rappelle l'importance de la directive SRI 2 récemment adoptée pour garantir un niveau plus élevé de cyberrésilience dans l'ensemble de l'Union; demande l'adoption et la mise en œuvre rapides d'actes d'exécution au titre de la présente directive afin de garantir que les fournisseurs de services de sécurité gérés respectent les exigences de la directive relatives aux mesures de gestion des risques en matière de cybersécurité;

5. recommande que les fournisseurs de services de sécurité gérés soient tenus de respecter les normes de cybersécurité pertinentes et fassent l'objet d'examens réguliers pour garantir la sécurité de leurs systèmes afin de protéger non seulement les fournisseurs eux-mêmes, mais aussi les entités qu'ils servent; estime que ces examens devraient évaluer la conformité des fournisseurs avec le cadre de certification de cybersécurité à l'échelle de l'Union ainsi que leur capacité à protéger contre les cybermenaces tant leurs systèmes que ceux de leurs clients;

6. se félicite de la proposition législative sur les services de sécurité gérés, qui vise à améliorer la qualité des services de sécurité gérés et à accroître leur comparabilité dans l'optique d'un bon fonctionnement du marché intérieur et de la mise en œuvre du marché unique numérique; souligne que la certification des services de sécurité gérés est pertinente dans le processus de sélection de la réserve de cybersécurité de l'UE et constitue également un indicateur de qualité et de confiance important pour les entités privées et publiques qui cherchent à acheter de tels services;

7. note que la proposition renforce le rôle de l'ENISA, qui devrait soutenir et promouvoir l'élaboration et la mise en œuvre de la politique de l'Union en matière de certification de cybersécurité des produits, services, processus et services de sécurité gérés dans le domaine des TIC, en surveillant régulièrement les évolutions dans les domaines connexes de la normalisation et en recommandant des spécifications techniques, lorsque des normes ne sont pas disponibles; propose que l'ENISA soit dotée d'une autorité et de ressources supplémentaires pour exercer sa mission élargie, y compris le financement de la recherche et du développement, ainsi qu'un mandat clair de coordination avec les agences nationales de cybersécurité et les acteurs du secteur; insiste sur le rôle essentiel des centres de réponse aux incidents de sécurité informatique (CSIRT) dans la mise en place d'un espace numérique prévisible et sûr pour les entreprises et les citoyens;

8. invite la Commission et l'ENISA à soutenir et à garantir une mise en œuvre cohérente du schéma européen de certification de cybersécurité que se fonde sur des règles non discriminatoires et reflète les normes européennes et internationales pour l'autoévaluation de la conformité par le fabricant ou le fournisseur de produits, services, processus ou services de sécurité gérés TIC, conformément au règlement de l'Union sur la cybersécurité; estime que cette mise en œuvre devrait contribuer à compenser les coûts de l'accréditation et encourager davantage de fabricants ou de fournisseurs à participer au système;

9. souligne que chaque système de certification devrait être conçu de manière à stimuler et à encourager tous les acteurs intervenant dans le secteur concerné à élaborer et à adopter des normes de sécurité, des normes techniques et des principes de sécurité dès la conception et de protection de la vie privée dès la conception, à tous les stades du cycle de vie du produit ou du service; souligne que les contributions de la société civile et des chercheurs indépendants, acteurs pertinents dans le domaine de la sécurité doivent être prises en compte de manière plus systématique lors de l'élaboration de ces principes; estime que les systèmes de certification devraient être cohérents avec les autres schémas européens de certification de cybersécurité adoptés conformément au règlement de l'Union sur la cybersécurité et devraient éviter de faire peser sur les fournisseurs une charge disproportionnée; recommande que les systèmes de certification comprennent des lignes directrices claires et détaillées sur la manière de mettre en œuvre les principes de sécurité dès la conception et de protection de la vie privée dès la conception, lorsque ces lignes directrices sont conformes aux dispositions établissant le cadre pour les schémas européens de cybersécurité dans le règlement de l'Union sur la cybersécurité; propose que, lorsque cela est nécessaire et proportionné, les systèmes de certification consistent en un mécanisme d'amélioration continue, comme des révisions et mises à jour régulières des normes de sécurité et des normes techniques; estime que le mécanisme devrait tenir compte des dernières évolutions en matière de menaces et de technologies en matière de cybersécurité; encourage à ce que chaque système de certification comprenne des mesures visant à promouvoir la transparence et la responsabilité, telles que la divulgation publique des résultats de la certification et des sanctions en cas de non-respect;

10. demande l'introduction d'un label de confiance de l'Union volontaire pour les produits, services, processus et services de sécurité gérés dans le domaine des TIC certifiés; souligne, à cet égard, que ce label pourrait contribuer à sensibiliser à la cybersécurité dans l'ensemble du marché intérieur et conférer ainsi un avantage concurrentiel aux entreprises disposant de bonnes qualifications en matière de cybersécurité; propose que le label de

confiance de l'Union soit conçu de manière à être facilement reconnaissable et compréhensible par les consommateurs et les entreprises;

11. recommande à la Commission et à l'ENISA de mettre en place un programme de recherche et de développement spécifique pour la cybersécurité; recommande à la Commission et à l'ENISA d'établir un cadre d'évaluation des risques en matière de cybersécurité pour les entreprises qui comprenne des lignes directrices sur la manière de recenser, d'évaluer et d'atténuer les risques en matière de cybersécurité, et pourrait être adapté aux différents secteurs et aux entreprises de différentes tailles; propose que la Commission et l'ENISA apportent une aide et une assistance aux États membres pour mettre en place un mécanisme de signalement des incidents de cybersécurité destiné aux consommateurs et aux entreprises, afin de faciliter la collecte de données sur les incidents de cybersécurité, lesquelles pourraient être utilisées pour améliorer les politiques et pratiques en matière de cybersécurité.

PROCÉDURE DE LA COMMISSION COMPÉTENTE AU FOND

Titre	Modification du règlement (UE) 2019/881 en ce qui concerne les services de sécurité gérés
Références	COM(2023)0208 – C9-0137/2023 – 2023/0108(COD)
Date de la présentation au PE	19.4.2023
Commission compétente au fond Date de l'annonce en séance	ITRE 1.6.2023
Commissions saisies pour avis Date de l'annonce en séance	IMCO LIBE 1.6.2023 1.6.2023
Avis non émis Date de la décision	LIBE 30.5.2023
Rapporteurs Date de la nomination	Josianne Cutajar 2.5.2023
Examen en commission	19.7.2023 19.9.2023
Date de l'adoption	25.10.2023
Résultat du vote final	+: 57 –: 0 0: 2
Membres présents au moment du vote final	Matteo Adinolfi, Nicola Beer, François-Xavier Bellamy, Hildegard Bentele, Tom Berendsen, Michael Bloss, Paolo Borchia, Marc Botenga, Markus Buchheit, Cristian-Silviu Buşoi, Jerzy Buzek, Maria da Graça Carvalho, Beatrice Covassi, Ciarán Cuffe, Josianne Cutajar, Nicola Danti, Marie Dauchy, Pilar del Castillo Vera, Christian Ehler, Lina Gálvez Muñoz, Jens Geier, Bart Groothuis, Christophe Grudler, Henrike Hahn, Ivo Hristov, Romana Jerković, Miapetra Kumpula-Natri, Thierry Mariani, Marina Mesure, Dan Nica, Niklas Nienass, Ville Niinistö, Johan Nissinen, Mauri Pekkarinen, Tsvetelina Penkova, Morten Petersen, Markus Pieper, Clara Ponsatí Obiols, Manuela Ripa, Sara Skyttedal, Riho Terras, Patrizia Toia, Henna Virkkunen, Pernille Weiss, Carlos Zorrinho
Suppléants présents au moment du vote final	Pascal Arimont, Tiziana Beghin, Franc Bogovič, Damien Carême, Martina Dlabajová, Francesca Donato, Matthias Ecke, Nicolás González Casares, Ladislav Ilčić, Luděk Niedermayer, Emma Wiesner
Suppléants (art. 209, par. 7) présents au moment du vote final	Asim Ademov, Aušra Maldeikienė, Irène Tolleret
Date du dépôt	26.10.2023

VOTE FINAL PAR APPEL NOMINAL EN COMMISSION COMPÉTENTE AU FOND

57	+
ECR	Ladislav Ilčić
ID	Matteo Adinolfi, Paolo Borchia, Marie Dauchy, Thierry Mariani
NI	Tiziana Beghin, Francesca Donato, Clara Ponsatí Obiols
PPE	Asim Ademov, Pascal Arimont, François-Xavier Bellamy, Hildegard Bentele, Tom Berendsen, Franc Bogovič, Cristian-Silviu Buşoi, Jerzy Buzek, Maria da Graça Carvalho, Pilar del Castillo Vera, Christian Ehler, Aušra Maldeikienė, Luděk Niedermayer, Markus Pieper, Sara Skyttedal, Riho Terras, Henna Virkkunen, Pernille Weiss
Renew	Nicola Beer, Nicola Danti, Martina Dlabajová, Bart Groothuis, Christophe Grudler, Mauri Pekkarinen, Morten Petersen, Irène Tolleret, Emma Wiesner
S&D	Beatrice Covassi, Josianne Cutajar, Matthias Ecke, Lina Gálvez Muñoz, Jens Geier, Nicolás González Casares, Ivo Hristov, Romana Jerković, Miapetra Kumpula-Natri, Dan Nica, Tsvetelina Penkova, Patrizia Toia, Carlos Zorrinho
The Left	Marc Botenga, Marina Mesure
Verts/ALE	Michael Bloss, Damien Carême, Ciarán Cuffe, Henrike Hahn, Niklas Nienass, Ville Niinistö, Manuela Ripa

0	-

2	0
ECR	Johan Nissinen
ID	Markus Buchheit

Légende des signes utilisés:
+ : pour
- : contre
0 : abstention