Parlement européen
2014-2019

Commission du marché intérieur et de la protection des consommateurs

2017/0225(COD)

22.5.2018

AVIS

de la commission du marché intérieur et de la protection des consommateurs

à l'intention de la commission de l'industrie, de la recherche et de l'énergie

sur la proposition de règlement du Parlement européen et du Conseil relatif à l'ENISA, Agence de l'Union européenne pour la cybersécurité, et abrogeant le règlement (UE) nº 526/2013, et relatif à la certification des technologies de l'information et des communications en matière de cybersécurité (règlement sur la cybersécurité)
(COM(2017)0477 – C8-0310-2017 – 2017/0225(COD))

Rapporteur pour avis: (*) Nicola Danti

(*) Commission associée – article 54 du règlement intérieur

PA_Legam

JUSTIFICATION SUCCINCTE

À l'ère du numérique, la cybersécurité est un élément essentiel pour la compétitivité économique et la sécurité de l'Union européenne, ainsi que pour l'intégrité de nos sociétés libres et démocratiques et les processus sur lesquels elles reposent. Garantir un niveau élevé de cyberrésilience dans toute l'Union est primordial pour gagner la confiance des consommateurs dans le marché numérique unique et pour poursuivre le développement vers une Europe plus innovante et plus compétitive.

Il ne fait aucun doute que les questions relatives aux cybermenaces et aux cyberattaques d'envergure mondiale, telles que «Wannacry» et «Meltdown», revêtent une importance croissante dans nos sociétés de plus en plus numérisées. Selon une enquête Eurobaromètre, publiée en juillet 2017, 87 % des répondants considèrent que la cybercriminalité «est un défi majeur à relever pour la sécurité intérieure de l'UE» et la majorité d'entre eux «craignent d'être victimes de différentes formes de cybercriminalité». En outre, depuis le début de l'année 2016, on dénombre plus de 4 000 attaques de rançongiciels par jour dans le monde, soit une hausse de 300 % depuis 2015, touchant 80 % d'entreprises européennes. Cet état de fait montre indéniablement qu'il est indispensable que l'Union soit plus résiliente et plus efficace dans son combat contre les cyberattaques et développe ses capacités pour mieux protéger les citoyens, les entreprises et les institutions publiques de l'Union.

Un an après l'entrée en vigueur de la directive sur la sécurité des réseaux et de l'information («directive SRI»), dans le cadre plus vaste de la stratégie de cybersécurité de l'Union européenne, la Commission européenne a présenté un règlement qui vise à renforcer la résilience, la dissuasion et la défense de l'Union dans le contexte des cyberattaques. Le 13 septembre 2017, la Commission a présenté le «règlement sur la cybersécurité» qui s'articule autour de deux piliers:
1) un mandat permanent et renforcé pour l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) pour aider les États membres à prévenir efficacement les cyberattaques et à y répondre et 2) la création d'un cadre de certification de cybersécurité de l'Union pour veiller à la cybersécurité des produits et services TIC.

Globalement, le rapporteur se félicite de la stratégie proposée par la Commission européenne, de même qu'il est favorable à l'établissement de systèmes de certification de cybersécurité à l'échelle de l'Union visant à améliorer la sécurité des produits et services TIC et à éviter la fragmentation coûteuse du marché unique dans ce domaine crucial. Même s'il est souhaitable que cet outil soit adopté, tout d'abord, sur une base volontaire, le rapporteur nourrit l'espoir de voir le cadre de certification de cybersécurité de l'Union et les procédures connexes devenir un outil indispensable pour rehausser la confiance de nos citoyens et des utilisateurs, et accroître la sécurité des produits et services qui circulent au sein du marché unique.

En effet, il est également convaincu que des précisions et des améliorations s'imposent sur plusieurs points de la proposition:

- premièrement et surtout, **associer davantage de parties prenantes concernées aux différentes phases du système de gouvernance dans le cadre de l'élaboration des systèmes candidats de certification par l'ENISA**: selon le rapporteur, il est essentiel de veiller à associer de manière formelle, les parties prenantes les plus concernées, telles que les secteurs des TIC, les associations de consommateurs, les PME, les organisations de normalisation de l'Union, les agences sectorielles de l'Union, etc. et de leur donner la possibilité de proposer de nouveaux systèmes candidats, de

conseiller l'ENISA grâce à leurs compétences ou de collaborer avec l'ESINA à l'élaboration d'un système candidat;

- deuxièmement, il convient de renforcer le rôle de coordination du groupe européen de certification de cybersécurité (composé des autorités nationales, avec l'appui de la Commission et de l'ENISA) grâce à de nouvelles missions consistant à fournir des orientations stratégiques et à **établir un programme de travail relatif aux actions communes à entreprendre au niveau de l'Union** dans le domaine de la certification, de même qu'à établir et à **mettre à jour régulièrement une liste prioritaire de produits et de services TIC** pour lesquels, selon le groupe, un système européen de certification de cybersécurité est requis.

- Le rapporteur est fermement convaincu que nous devrions éviter la pratique du «shopping» pour la certification de l'Union, comme cela s'est déjà produit dans d'autres secteurs. Les **dispositions en matière de contrôle et de surveillance de l'ENISA et des autorités nationales de contrôle de la certification devraient être considérablement renforcées**, afin de garantir qu'un certificat européen délivré dans un État membre offrira des normes et des exigences identiques que celui délivré dans un autre État membre. En conséquence, il propose:

  1) de renforcer les pouvoirs de surveillance de l'ENISA: avec le groupe de certification, l'ENISA devrait procéder à des évaluations des procédures mises en place par les autorités chargées de délivrer des certificats de l'Union;
  2) que les autorités nationales de contrôle de la certification devraient procéder à des évaluations régulières (au moins tous les deux ans) des certificats de l'Union délivrés par les organismes d'évaluation de la conformité;
  3) d'introduire des critères contraignants communs à définir par le groupe afin de déterminer l'ampleur, de la portée et de la fréquence des évaluations, visées au point 2, auxquelles les autorités nationales de contrôle de la certification devraient procéder.

- Le rapporteur estime qu'un **label de confiance de l'Union européenne** devrait être introduit pour les produits et services TIC certifiés et destinés aux utilisateurs finals. Ce label pourrait contribuer à sensibiliser à la cybersécurité et donner un avantage concurrentiel aux entreprises possédant de bonnes références en matière de cybersécurité.

- Le rapporteur souscrit à la stratégie uniforme et harmonisée adoptée par la Commission, mais il est convaincu qu'elle devrait être plus flexible et adaptable aux caractéristiques et vulnérabilités de chaque produit ou service: non au principe d'«une solution universelle pour toutes les situations». Dès lors, le rapporteur estime que les **niveaux d'assurance** devraient être renommés et utilisés en tenant compte de l'utilisation prévue des produits et services TIC. De la même façon, la durée de **validité du certificat** est à définir selon le système concerné.

- Chaque système européen 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.

AMENDEMENTS

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 amendements suivants:

Amendement 1

Proposition de règlement
Considérant 1

Texte proposé par la Commission	*Amendement*
(1) Les réseaux et systèmes d'information et les réseaux et services de télécommunications remplissent une fonction essentielle pour la société et sont devenus le nerf de la croissance économique. Les technologies de l'information et des communications sont le fondement des systèmes complexes qui rendent possibles les activités sociales; elles permettent à nos économies de fonctionner dans des secteurs clés comme la santé, l'énergie, la finance et les transports, et soutiennent en particulier le fonctionnement du marché intérieur.	(1) Les réseaux et systèmes d'information et les réseaux et services de télécommunications remplissent une fonction essentielle pour la société et sont devenus le nerf de la croissance économique. Les technologies de l'information et des communications ***(TIC)*** sont le fondement des systèmes complexes qui rendent possibles les activités sociales ***courantes;*** elles permettent à nos économies de fonctionner dans des secteurs clés comme la santé, l'énergie, la finance et les transports, et soutiennent en particulier le fonctionnement du marché intérieur.

Amendement 2

Proposition de règlement
Considérant 2

Texte proposé par la Commission	*Amendement*
(2) L'utilisation des réseaux et des systèmes d'information par les particuliers, les entreprises et les pouvoirs publics s'est généralisée dans l'Union tout entière. La numérisation et la connectivité caractérisent un nombre toujours croissant de produits et de services; avec l'avènement de l'internet des objets (IdO), ce sont des millions, sinon des milliards, de dispositifs numériques connectés qui devraient être mis en service dans l'UE au cours de la prochaine décennie. Alors	(2) L'utilisation des réseaux et des systèmes d'information par les particuliers, les entreprises et les pouvoirs publics s'est généralisée dans l'Union tout entière. La numérisation et la connectivité caractérisent un nombre toujours croissant de produits et de services; avec l'avènement de l'internet des objets (IdO), ce sont des millions, sinon des milliards, de dispositifs numériques connectés qui devraient être mis en service dans l'UE au cours de la prochaine décennie. Alors

qu'un nombre croissant de dispositifs sont connectés à l'internet, leur conception n'intègre pas suffisamment les impératifs de sécurité et de résilience, de sorte que la cybersécurité est insuffisante. Dans ce contexte, le recours limité à la certification entraîne un manque d'information des utilisateurs, qu'il s'agisse de particuliers ou d'organisations, sur les caractéristiques des produits et services TIC en matière de cybersécurité, sapant ainsi la confiance dans les solutions numériques.

qu'un nombre croissant de dispositifs sont connectés à l'internet, leur conception n'intègre pas suffisamment les impératifs de sécurité et de résilience, de sorte que la cybersécurité est insuffisante. Dans ce contexte, le recours limité à la certification entraîne un manque d'information des utilisateurs, qu'il s'agisse de particuliers ou d'organisations, sur les caractéristiques des produits et services TIC en matière de cybersécurité, sapant ainsi la confiance dans les solutions numériques pourtant ***essentielle à la mise en place du marché unique numérique***.

Amendement 3

Proposition de règlement
Considérant 3

Texte proposé par la Commission

(3) Une numérisation et une connectivité accrues entraînent une augmentation des risques en matière de cybersécurité, ce qui rend ainsi l'ensemble de la société plus vulnérable aux cybermenaces et exacerbe les dangers auxquels sont confrontés les individus, notamment les personnes vulnérables telles que les enfants. Afin d'atténuer ***ce risque*** pour la société, il convient de prendre toutes les mesures nécessaires pour améliorer la ***cybersécurité*** dans l'Union afin de mieux protéger les réseaux et systèmes d'information, les réseaux de télécommunication, les produits, services et appareils numériques utilisés par les particuliers, les pouvoirs publics et les entreprises — depuis les PME jusqu'aux opérateurs d'infrastructures critiques — contre les cybermenaces.

Amendement

(3) Une numérisation et une connectivité accrues entraînent une augmentation ***majeure*** des risques en matière de cybersécurité, ce qui rend ainsi l'ensemble de la société plus vulnérable aux cybermenaces et exacerbe les dangers auxquels sont confrontés les individus, notamment les personnes vulnérables telles que les enfants. ***Le pouvoir de transformation de l'intelligence artificielle et de l'apprentissage automatique sera exploité par l'ensemble de la société, et donc aussi par les cybercriminels.*** Afin d'atténuer ***ces risques*** pour la société, il convient de prendre toutes les mesures nécessaires pour améliorer la ***sécurité contre les cyberattaques*** dans l'Union***,*** afin de mieux protéger les réseaux et systèmes d'information, les réseaux de télécommunication, les produits, services et appareils numériques utilisés par les particuliers, les pouvoirs publics et les entreprises — depuis les PME jusqu'aux opérateurs d'infrastructures critiques —

contre les cybermenaces.

Amendement 4

Proposition de règlement
Considérant 4

Texte proposé par la Commission	*Amendement*
(4) Les cyberattaques sont en augmentation; une économie et une société connectées, qui sont plus vulnérables aux cybermenaces et aux cyberattaques, ont donc besoin de dispositifs de défense renforcés. Cependant, alors que les cyberattaques sont souvent de nature transnationale, les réponses apportées par les autorités chargées de la cybersécurité et les compétences en matière de répression sont surtout nationales. Des incidents de cybersécurité majeurs pourraient perturber la fourniture de services essentiels dans l'ensemble de l'UE. Il est donc indispensable de mettre sur pied une capacité de réaction et de gestion des crises à l'échelon de l'UE, sur la base de politiques spécifiques et d'instruments élargis aux fins de la solidarité européenne et de l'assistance mutuelle. En outre, il est important pour les décideurs, les entreprises et les utilisateurs que la situation en matière de cybersécurité et de résilience dans l'Union soit régulièrement évaluée à partir de données de l'Union fiables et d'une anticipation systématique des évolutions, défis et menaces futurs tant au niveau de l'Union qu'au niveau mondial.	(4) Les cyberattaques sont en augmentation; une économie et une société connectées, qui sont plus vulnérables aux cybermenaces et aux cyberattaques, ont donc besoin de dispositifs de défense renforcés ***et plus sûrs***. Cependant, alors que les cyberattaques sont souvent de nature transnationale, les réponses apportées par les autorités chargées de la cybersécurité et les compétences en matière de répression sont surtout nationales. Des incidents de cybersécurité majeurs pourraient perturber la fourniture de services essentiels dans l'ensemble de l'UE. Il est donc indispensable de mettre sur pied une capacité de réaction et de gestion des crises à l'échelon de l'UE, sur la base de politiques spécifiques et d'instruments élargis aux fins de la solidarité européenne et de l'assistance mutuelle. En outre, il est important pour les décideurs, les entreprises et les utilisateurs que la situation en matière de cybersécurité et de résilience dans l'Union soit régulièrement évaluée à partir de données de l'Union fiables et d'une anticipation systématique des évolutions, défis et menaces futurs tant au niveau de l'Union qu'au niveau mondial.

Amendement 5

Proposition de règlement
Considérant 5

Texte proposé par la Commission	*Amendement*
(5) Compte tenu de l'augmentation des	(5) Compte tenu de l'augmentation des

enjeux auxquels l'Union est confrontée dans le domaine de la cybersécurité, il est nécessaire de disposer d'une panoplie de mesures qui développent les actions déjà menées par l'Union et promeuvent des objectifs se renforçant mutuellement. Ces objectifs sont notamment la nécessité de continuer à renforcer les capacités et l'état de préparation des États membres et des entreprises, ainsi que d'améliorer la coopération et la coordination entre les États membres et les institutions, organes et organismes de l'UE. En outre, étant donné la nature universelle des cybermenaces, il est nécessaire d'augmenter, au niveau de l'Union, les capacités susceptibles de compléter l'action des États membres, notamment dans les cas d'incidents et crises transfrontières de cybersécurité majeurs. Des efforts supplémentaires sont également requis pour sensibiliser davantage les particuliers et les entreprises aux questions de cybersécurité. En outre, ***une information transparente sur le niveau*** de ***sécurité qui caractérise les produits et services TIC permettrait*** de renforcer la confiance ***dans*** le ***marché unique numérique***. Une certification mise en œuvre à l'échelle de ***l'UE***, prévoyant des exigences et des critères d'évaluation communs en matière de cybersécurité dans l'ensemble des marchés nationaux et des secteurs, peut faciliter cette transparence.

enjeux auxquels l'Union est confrontée dans le domaine de la cybersécurité, il est nécessaire de disposer d'une panoplie de mesures qui développent les actions déjà menées par l'Union et promeuvent des objectifs se renforçant mutuellement. Ces objectifs sont notamment la nécessité de continuer à renforcer les capacités et l'état de préparation des États membres et des entreprises, ainsi que d'améliorer la coopération et la coordination entre les États membres et les institutions, organes et organismes de l'UE. En outre, étant donné la nature universelle des cybermenaces, il est nécessaire d'augmenter, au niveau de l'Union, les capacités susceptibles de compléter l'action des États membres, notamment dans les cas d'incidents et crises transfrontières de cybersécurité majeurs. Des efforts supplémentaires sont également requis pour sensibiliser davantage les particuliers et les entreprises aux questions de cybersécurité. En outre, ***étant donné que les cyberincidents ébranlent la confiance vis-à-vis des fournisseurs*** de ***services numériques et dans le marché numérique unique lui-même, notamment chez les consommateurs, il est souhaitable*** de renforcer la confiance ***en offrant des informations transparentes sur*** le ***niveau de sécurité des produits et services TIC***. Une certification mise en œuvre à l'échelle de ***l'Union***, ***fondée sur des normes européennes ou internationales et*** prévoyant des exigences et des critères d'évaluation communs en matière de cybersécurité dans l'ensemble des marchés nationaux et des secteurs, peut faciliter cette transparence. ***Parallèlement à la certification à l'échelle de l'Union, il existe un ensemble de mesures volontaires que le secteur privé devrait adopter lui-même, afin de rehausser la confiance dans la sécurité des produits et services TIC, notamment en considération de la disponibilité croissante de dispositifs de l'internet des objets (IdO). Par exemple, il conviendrait de s'appuyer davantage sur***

les technologies de cryptage et autres, ainsi que sur des technologies visant à empêcher la réussite des cyberattaques, telles que la chaîne de blocs, pour améliorer la sécurité des données et des communications des utilisateurs finals et la sécurité globale des réseaux et des systèmes d'information dans l'Union.

Amendement 6

Proposition de règlement
Considérant 5 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	(5 bis) Si la certification et les autres formes d'évaluation de la conformité des processus, produits et services TIC jouent un rôle important, l'amélioration de la cybersécurité demande une approche plurielle englobant les individus, les processus et les technologies. L'Union européenne devrait également continuer de valoriser et de promouvoir d'autres efforts, dont l'éducation, la formation et le développement des compétences en matière de cybersécurité, la sensibilisation à ce sujet auprès des directions exécutives et des conseils d'administration des entreprises, la promotion du partage volontaire d'informations sur les cybermenaces, et la transition d'une approche réactive à une approche anticipative de la réponse aux menaces en valorisant la prévention des cyberattaques.

Amendement 7

Proposition de règlement
Considérant 7

Texte proposé par la Commission	*Amendement*
(7) L'Union a déjà pris d'importantes mesures pour garantir la cybersécurité et	(7) L'Union a déjà pris d'importantes mesures pour garantir la cybersécurité et

renforcer la confiance dans les technologies numériques. En 2013, l'UE s'est dotée d'une stratégie de cybersécurité afin d'orienter la politique qu'elle entendait mener en réaction aux menaces et aux risques qui pèsent sur la cybersécurité. Dans le cadre de ses efforts pour mieux protéger les Européens en ligne, l'Union a adopté en 2016 le premier acte législatif dans le domaine de la cybersécurité, la directive (UE) 2016/1148 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union (la «directive SRI»). La directive SRI a instauré des exigences concernant les capacités nationales dans le domaine de la cybersécurité, établi le premier mécanisme destiné à améliorer la coopération stratégique et opérationnelle entre les États membres, et introduit des obligations concernant les mesures de sécurité et la notification des incidents dans différents secteurs qui revêtent une importance vitale pour l'économie et la société, tels que l'énergie, les transports, l'eau, les banques, les infrastructures des marchés financiers, les soins de santé, les infrastructures numériques ainsi que les fournisseurs de services numériques fondamentaux (moteurs de recherche, services d'informatique en nuage et places de marché en ligne). L'ENISA s'est vu attribuer un rôle essentiel d'appui à la mise en œuvre de cette directive. En outre, lutter efficacement contre la cybercriminalité est l'une des principales priorités du programme européen en matière de sécurité et contribue à l'objectif global consistant à atteindre un niveau élevé de cybersécurité.

renforcer la confiance dans les technologies numériques. En 2013, l'UE s'est dotée d'une stratégie de cybersécurité afin d'orienter la politique qu'elle entendait mener en réaction aux menaces et aux risques qui pèsent sur la cybersécurité. Dans le cadre de ses efforts pour mieux protéger les Européens en ligne, l'Union a adopté en 2016 le premier acte législatif dans le domaine de la cybersécurité, la directive (UE) 2016/1148 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union (la «directive SRI»). La directive SRI***, dont le succès dépendra dans une large mesure de la mise en œuvre effective par les États membres,*** a instauré des exigences concernant les capacités nationales dans le domaine de la cybersécurité, établi le premier mécanisme destiné à améliorer la coopération stratégique et opérationnelle entre les États membres, et introduit des obligations concernant les mesures de sécurité et la notification des incidents dans différents secteurs qui revêtent une importance vitale pour l'économie et la société, tels que l'énergie, les transports, l'eau, les banques, les infrastructures des marchés financiers, les soins de santé, les infrastructures numériques ainsi que les fournisseurs de services numériques fondamentaux (moteurs de recherche, services d'informatique en nuage et places de marché en ligne). L'ENISA s'est vu attribuer un rôle essentiel d'appui à la mise en œuvre de cette directive. En outre, lutter efficacement contre la cybercriminalité est l'une des principales priorités du programme européen en matière de sécurité et contribue à l'objectif global consistant à atteindre un niveau élevé de cybersécurité.

Amendement 8

Proposition de règlement
Considérant 11

Texte proposé par la Commission	*Amendement*
(11) Étant donné l'aggravation des défis en matière de cybersécurité auxquels l'Union est confrontée, il faudrait augmenter les ressources financières et humaines allouées à l'Agence pour tenir compte du renforcement de son rôle et de ses missions, ainsi que de sa position critique parmi les organisations qui défendent l'écosystème numérique européen.	(11) Étant donné l'aggravation des ***menaces et des*** défis en matière de cybersécurité auxquels l'Union est confrontée, il faudrait augmenter les ressources financières et humaines allouées à l'Agence pour tenir compte du renforcement de son rôle et de ses missions, ainsi que de sa position critique parmi les organisations qui défendent l'écosystème numérique européen.

Amendement 9

Proposition de règlement
Considérant 28

Texte proposé par la Commission	*Amendement*
(28) L'Agence devrait contribuer à sensibiliser le public aux risques liés à la cybersécurité et fournir, à l'intention des particuliers et des organisations, des orientations sur les bonnes pratiques à adopter par les utilisateurs. L'Agence devrait également contribuer à promouvoir les meilleures pratiques et solutions ***pour*** les particuliers et les organisations ***en collectant*** et ***en analysant*** des informations du domaine public sur les incidents significatifs, et ***en rédigeant*** des rapports en vue de fournir des orientations aux entreprises et aux particuliers, et d'améliorer le niveau global de préparation et de résilience. L'Agence devrait en outre organiser, en coopération avec les membres et les institutions, organes et organismes de l'Union, des campagnes d'information régulières et des campagnes publiques d'éducation s'adressant aux utilisateurs finals, en vue de promouvoir une navigation en ligne plus sûre pour tous et de sensibiliser aux dangers potentiels du cyberespace, y compris la cybercriminalité notamment ***sous forme d'hameçonnages***, réseaux zombies, fraudes financières et	(28) L'Agence devrait contribuer à sensibiliser le public aux risques liés à la cybersécurité et fournir, à l'intention des particuliers et des organisations, des orientations sur les bonnes pratiques à adopter par les utilisateurs. L'agence devrait également contribuer à promouvoir les meilleures pratiques et solutions ***en matière d'hygiène cybernétique, à savoir des mesures de routine simples que*** les particuliers et les organisations ***peuvent prendre afin de minimiser les risques liés aux cybermenaces, telles que l'authentification multifactorielle, les correctifs, le cryptage*** et ***la gestion*** des ***accès; À cette fin, l'Agence devrait également collecter et analyser les*** informations du domaine public sur les incidents significatifs, et ***rédiger et publier et*** des rapports ***et des guides*** en vue de fournir des orientations aux entreprises et aux particuliers, et d'améliorer le niveau global de préparation et de résilience. L'Agence devrait en outre organiser, en coopération avec les membres et les institutions, organes et organismes de l'Union, des campagnes d'information

bancaires, et de donner des conseils de base en ***matière d'authentification et*** de protection des données. L'Agence devrait jouer un rôle central dans l'accélération de la sensibilisation des utilisateurs finals à la sécurité des appareils.

régulières et des campagnes publiques d'éducation s'adressant aux utilisateurs finals, en vue de promouvoir une navigation en ligne plus sûre pour tous et de sensibiliser aux ***mesures pouvant être prises pour se prémunir contre les*** dangers potentiels du cyberespace, y compris la cybercriminalité notamment***, tels que les hameçonnages, les rançongiciels, le piratage***, ***les*** réseaux zombies, ***les*** fraudes financières et bancaires, et de donner des conseils de base en ***ce qui concerne l'authentification multifactorielle, le cryptage, les correctifs, les principes*** de ***la gestion des accès, la*** protection des données ***et les autres technologies améliorant la sécurité et la protection de la vie privée et les outils d'anonymisation***. L'Agence devrait jouer un rôle central dans l'accélération de la sensibilisation des utilisateurs finals à la sécurité des appareils et assurer une utilisation sûre des services***, en développant la sécurité dès la conception au niveau de l'Union, ce qui est d'une importance capitale pour améliorer la sécurité des appareils connectés, en particulier à l'intention des utilisateurs finals vulnérables, notamment les enfants, ainsi que la protection de la vie privée dès la conception. L'Agence devrait encourager tous les utilisateurs finals à prendre les mesures appropriées pour prévenir et minimiser les conséquences des incidents compromettant la sécurité de leurs réseaux et de leurs systèmes d'information. Des partenariats devraient être noués avec des établissements universitaires menant des initiatives de recherche dans les domaines concernés de la cybersécurité.***

Amendement 10

Proposition de règlement
Considérant 35

Texte proposé par la Commission	*Amendement*
(35) L'Agence devrait encourager les États membres et les fournisseurs de services à renforcer leurs normes de sécurité générales, de manière que tous les utilisateurs d'internet puissent prendre les mesures nécessaires pour garantir leur propre cybersécurité. En particulier, les fournisseurs de services et les fabricants de produits devraient retirer ou recycler les produits et services qui ne satisfont pas aux normes de cybersécurité. En coopération avec les autorités compétentes, l'ENISA peut diffuser des informations sur le niveau de cybersécurité des produits et services offerts sur le marché intérieur, et émettre des alertes visant des fournisseurs et des fabricants et les contraignant à améliorer la sécurité de leurs produits et services, y compris leur cybersécurité.	(35) L'Agence devrait encourager les États membres et les fournisseurs de services à renforcer leurs normes de sécurité générales, de manière que tous les utilisateurs d'internet puissent prendre les mesures nécessaires pour garantir leur propre cybersécurité. En particulier, les fournisseurs de services et les fabricants de produits devraient retirer ou recycler les produits et services qui ne satisfont pas aux normes de cybersécurité. En coopération avec les autorités compétentes, l'ENISA peut diffuser des informations sur le niveau de cybersécurité des produits et services offerts sur le marché intérieur, et émettre des alertes visant des fournisseurs et des fabricants et les contraignant à améliorer la sécurité de leurs produits et services, y compris leur cybersécurité. ***L'ENISA devrait publier ces alertes sur le site web destiné à la diffusion d'informations relatives aux systèmes de certification. L'Agence devrait élaborer des lignes directrices sur les exigences de sécurité minimales applicables aux équipements informatiques vendus au sein de l'Union ou exportés à partir de l'Union. Ces lignes directrices pourraient imposer aux fabricants de fournir une déclaration écrite certifiant que l'équipement ne contient aucun composant matériel, logiciel ou micrologiciel comportant une vulnérabilité connue en matière de sécurité ni aucun mot de passe ou code d'accès non crypté ou non modifiable, qu'il peut accepter des mises à jour de sécurité dûment authentifiées et fiables, que la réponse apportée par les vendeurs en ce qui concerne l'équipement en question prévoit une hiérarchie appropriée de mesures correctives et que les vendeurs informent les utilisateurs finals de la date de fin de l'assistance pour l'équipement en matière de sécurité.***

Amendement 11

Proposition de règlement
Considérant 36 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	(36 bis) Les normes constituent un instrument volontaire, ajusté aux conditions du marché, offrant des exigences et des conseils techniques et découlant d'un processus ouvert, transparent et exhaustif. Le recours aux normes facilite la conformité des biens et services à la législation de l'Union et soutient les politiques européennes conformément au règlement (UE) nº 1025/2012 relatif à la normalisation européenne. L'Agence devrait consulter régulièrement les organisations européennes de normalisation et collaborer avec eux, notamment lors de l'élaboration des systèmes européens de certification de cybersécurité.

Amendement 12

Proposition de règlement
Considérant 44

Texte proposé par la Commission	*Amendement*
(44) L'Agence devrait disposer, à titre d'organe consultatif, d'un groupe permanent des parties prenantes pour maintenir un dialogue régulier avec le secteur privé, les organisations de consommateurs et les autres parties prenantes. Le groupe permanent des parties prenantes, institué par le conseil d'administration sur proposition du directeur exécutif, devrait s'attacher à examiner des questions pertinentes pour les parties prenantes et à les porter à l'attention de l'Agence. La composition du groupe permanent des parties prenantes et les tâches assignées à ce groupe, qui doit être consulté en particulier sur le projet de	(44) L'Agence devrait disposer, à titre d'organe consultatif, d'un groupe permanent des parties prenantes pour maintenir un dialogue régulier avec le secteur privé, les organisations de consommateurs***, le monde universitaire*** et les autres parties prenantes. Le groupe permanent des parties prenantes, institué par le conseil d'administration sur proposition du directeur exécutif, devrait s'attacher à examiner des questions pertinentes pour les parties prenantes et à les porter à l'attention de l'Agence. ***Afin d'assurer une participation adéquate de parties prenantes dans le cadre de la certification de cybersécurité, le groupe***

programme de travail, devraient assurer une représentation ***suffisante*** des parties prenantes dans le travail de l'Agence.

permanent des parties prenantes devrait également apporter ses conseils sur les produits et services TIC qui doivent être couverts dans les futurs systèmes européens de certification de cybersécurité, et devrait présenter des propositions à la Commission pour demander à l'agence d'élaborer des systèmes candidats sur ces produits et services TIC, à son initiative ou dans le sillage de propositions émanant de parties prenantes concernées. La composition du groupe permanent des parties prenantes et les tâches assignées à ce groupe, qui doit être consulté en particulier sur le projet de programme de travail, devraient assurer une représentation ***judicieuse et équitable*** des parties prenantes dans le travail de l'Agence.

Amendement 13

Proposition de règlement
Considérant 46

Texte proposé par la Commission	*Amendement*
(46) Pour garantir l'autonomie et l'indépendance complètes de l'Agence et lui permettre d'effectuer des missions nouvelles et supplémentaires, y compris des missions urgentes imprévues, il conviendrait de la doter d'un budget suffisant et autonome dont l'essentiel des recettes provienne d'une contribution de l'Union et de contributions des pays tiers participant aux travaux de l'Agence. La plus grande partie des effectifs de l'Agence devrait se consacrer directement à la mise en œuvre opérationnelle du mandat de l'Agence. L'État membre d'accueil ou tout autre État membre devrait être autorisé à apporter des contributions volontaires aux recettes de l'Agence. La procédure budgétaire de l'Union devrait rester applicable en ce qui concerne toute subvention imputable sur le budget général de l'Union. En outre, la Cour des comptes devrait contrôler les comptes de l'Agence	(46) Pour garantir l'autonomie et l'indépendance complètes de l'Agence et lui permettre d'effectuer des missions nouvelles et supplémentaires, y compris des missions urgentes imprévues, il conviendrait de la doter d'un budget suffisant et autonome dont l'essentiel des recettes provienne d'une contribution de l'Union et de contributions des pays tiers participant aux travaux de l'Agence. La plus grande partie des effectifs de l'Agence devrait se consacrer directement à la mise en œuvre opérationnelle du mandat de l'Agence. L'État membre d'accueil ou tout autre État membre devrait être autorisé à apporter des contributions volontaires aux recettes de l'Agence. La procédure budgétaire de l'Union devrait rester applicable en ce qui concerne toute subvention imputable sur le budget général de l'Union. En outre, la Cour des comptes devrait contrôler les comptes de l'Agence

afin de garantir la transparence ***et*** la responsabilité.

afin de garantir la transparence***,*** la responsabilité***, l'efficacité et l'adéquation des crédits engagés***.

Amendement 14

Proposition de règlement
Considérant 47

Texte proposé par la Commission

(47) L'évaluation de la conformité est le processus destiné à établir si les exigences spécifiées relatives à un produit, à un processus, à un service, à un système, à une personne ou à un organisme ont été respectées. Aux fins du présent règlement, il y a lieu de considérer la certification comme un type d'évaluation de la conformité portant sur les caractéristiques de cybersécurité d'un produit, processus, service, système, ou d'une combinaison de ceux-ci («produits et services TIC») effectuée par un tiers indépendant***, distinct du fabricant du produit ou du fournisseur du service***. En soi, la certification ne peut garantir que les produits et services TIC certifiés sont fiables du point de vue de la cybersécurité. Il s'agit plutôt d'une procédure et d'une méthodologie technique visant à attester que des produits et services TIC ont été soumis à des essais et qu'ils sont conformes à certaines exigences de cybersécurité définies par ailleurs, par exemple dans des normes techniques.

Amendement

(47) L'évaluation de la conformité est le processus destiné à établir si les exigences spécifiées relatives à un produit, à un processus, à un service, à un système, à une personne ou à un organisme ont été respectées. Aux fins du présent règlement, il y a lieu de considérer la certification comme un type d'évaluation de la conformité portant sur les caractéristiques ***et les pratiques*** de cybersécurité d'un produit, processus, service, système, ou d'une combinaison de ceux-ci («produits et services TIC») effectuée par un tiers indépendant ***ou au moyen d'une procédure d'autodéclaration de conformité***. En soi, la certification ne peut garantir que les produits et services TIC certifiés sont fiables du point de vue de la cybersécurité; ***il conviendrait d'y sensibiliser l'utilisateur final***. Il s'agit plutôt d'une procédure et d'une méthodologie technique visant à attester que des produits et services TIC, ***ainsi que les processus et systèmes sous-jacents*** ont été soumis à des essais et qu'ils sont conformes à certaines exigences de cybersécurité définies par ailleurs, par exemple dans des normes techniques.

Amendement 15

Proposition de règlement
Considérant 48

Texte proposé par la Commission

Amendement

(48) La certification de cybersécurité est ***importante*** pour accroître la sécurité des produits et services et renforcer la confiance qui leur est accordée. Le marché unique numérique, et en particulier l'économie des données et l'internet des objets, ne peuvent prospérer que si le grand public est convaincu que ces produits et services offrent un ***certain*** niveau d'assurance de cybersécurité. Les voitures connectées et automatisées, les dispositifs médicaux électroniques, les systèmes de contrôle-commande industriels ou les réseaux intelligents ne sont que quelques exemples de secteurs dans lesquels la certification est déjà largement utilisée ou est susceptible de l'être dans un avenir proche. Les secteurs régis par la directive SRI sont également des secteurs où la certification de cybersécurité joue un rôle critique.

(48) La certification ***européenne*** de cybersécurité est ***essentielle*** pour accroître la sécurité des produits et services et renforcer la confiance qui leur est accordée. Le marché unique numérique, et en particulier l'économie des données et l'internet des objets, ne peuvent prospérer que si le grand public est convaincu que ces produits et services offrent un niveau d'assurance de cybersécurité ***élevé***. Les voitures connectées et automatisées, les dispositifs médicaux électroniques, les systèmes de contrôle-commande industriels ou les réseaux intelligents ne sont que quelques exemples de secteurs dans lesquels la certification est déjà largement utilisée ou est susceptible de l'être dans un avenir proche. Les secteurs régis par la directive SRI sont également des secteurs où la certification de cybersécurité joue un rôle critique.

Amendement 16

Proposition de règlement
Considérant 50

Texte proposé par la Commission

(50) Actuellement, la certification de cybersécurité des produits et services TIC n'est utilisée que de façon limitée. Lorsqu'elle existe, elle intervient généralement au niveau des États membres ou dans le cadre de systèmes pilotés par l'industrie. Dans ce contexte, un certificat délivré par une autorité nationale de cybersécurité n'est pas, en principe, reconnu par d'autres États membres. Il arrive donc que les entreprises doivent certifier leurs produits et services dans les différents États membres où elles exercent leurs activités, par exemple pour participer à des procédures nationales de passation de marchés. En outre, alors que de nouveaux systèmes voient le jour, il ne semble pas exister d'approche cohérente et globale des questions de cybersécurité transversales,

Amendement

(50) Actuellement, la certification de cybersécurité des produits et services TIC n'est utilisée que de façon limitée. Lorsqu'elle existe, elle intervient généralement au niveau des États membres ou dans le cadre de systèmes pilotés par l'industrie. Dans ce contexte, un certificat délivré par une autorité nationale de cybersécurité n'est pas, en principe, reconnu par d'autres États membres. Il arrive donc que les entreprises doivent certifier leurs produits et services dans les différents États membres où elles exercent leurs activités, par exemple pour participer à des procédures nationales de passation de marchés***, ce qui peut entraîner des surcoûts pour elles***. En outre, alors que de nouveaux systèmes voient le jour, il ne semble pas exister d'approche cohérente et

par exemple dans le domaine de l'internet des objets. Les systèmes existants présentent des lacunes importantes et des différences en termes de couverture des produits, de niveau d'assurance, de critères de fond et d'utilisation effective.

globale des questions de cybersécurité transversales, par exemple dans le domaine de l'internet des objets. Les systèmes existants présentent des lacunes importantes et des différences en termes de couverture des produits, de niveau d'assurance ***fondée sur le risque***, de critères de fond et d'utilisation effective.

Amendement 17

Proposition de règlement
Considérant 52

Texte proposé par la Commission

(52) Compte tenu de ce qui précède, il est nécessaire d'établir un cadre européen de certification de cybersécurité définissant les principales exigences horizontales pour les systèmes de certification de cybersécurité à développer, et permettant la reconnaissance et l'utilisation dans tous les États membres des certificats applicables aux produits et services TIC. Le cadre européen devrait poursuivre un double objectif. D'une part, il devrait contribuer à rehausser la confiance dans les produits et services TIC qui ont été certifiés conformément à de tels systèmes. D'autre part, il devrait éviter la multiplication de certifications de cybersécurité nationales contradictoires ou faisant double emploi, ce qui réduirait les coûts à charge des entreprises opérant dans le marché unique numérique. Les systèmes devraient être non discriminatoires et fondés sur des normes internationales et/ou européennes, sauf si ces normes sont inefficaces ou inappropriées pour remplir les objectifs légitimes de l'UE à cet égard.

Amendement

(52) Compte tenu de ce qui précède, il est nécessaire ***d'adopter une approche commune et*** d'établir un cadre européen de certification de cybersécurité définissant les principales exigences horizontales pour les systèmes de certification de cybersécurité à développer, et permettant la reconnaissance et l'utilisation dans tous les États membres des certificats applicables aux produits et services TIC. ***Ce faisant, il est essentiel de s'appuyer sur des systèmes nationaux et internationaux existants, ainsi que sur des systèmes de reconnaissance mutuelle, notamment du SOG-IS (groupe de hauts fonctionnaires pour la sécurité des systèmes d'information) et de créer les conditions d'une transition en douceur entre les systèmes existants relevant de ces systèmes et les systèmes relevant du nouveau cadre européen.*** Le cadre européen devrait poursuivre un double objectif. D'une part, il devrait contribuer à rehausser la confiance dans les produits et services TIC qui ont été certifiés conformément à de tels systèmes. D'autre part, il devrait éviter la multiplication de certifications de cybersécurité nationales contradictoires ou faisant double emploi, ce qui réduirait les coûts à charge des entreprises opérant dans le marché unique numérique. ***Lorsqu'une certification***

européenne de cybersécurité a remplacé un système national, les certificats délivrés au titre du système européen devraient être considérés comme valables dans les cas où une certification au titre du système national était requise. Les systèmes devraient ***s'inspirer de la sécurité dès la conception et des principes énoncés dans le règlement (UE) 2016/679. Ils devraient également*** être non discriminatoires et fondés sur des normes internationales et/ou européennes, sauf si ces normes sont inefficaces ou inappropriées pour remplir les objectifs légitimes de l'UE à cet égard.

Amendement 18

Proposition de règlement
Considérant 52 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	(52 bis) Ce cadre européen de certification de cybersecurité devrait être établi de manière homogène dans tous les États membres afin d'éviter la pratique du «shopping de certifications» en raison de différences de coûts ou de niveaux d'exigence entre les États membres.

Amendement 19

Proposition de règlement
Considérant 55

Texte proposé par la Commission	*Amendement*
(55) Les systèmes européens de certification de cybersécurité devraient avoir pour finalité de garantir que les produits et services TIC certifiés selon un tel système sont conformes aux exigences spécifiées. Ces exigences concernent l'aptitude à résister, à un niveau d'assurance donné, aux actions qui visent à compromettre la disponibilité,	(55) Les systèmes européens de certification de cybersécurité devraient avoir pour finalité de ***contribuer à un niveau de protection élevé de l'utilisateur final et de la compétitivité européenne et de renforcer le niveau de sécurité au sein du marché unique numérique, et plus particulièrement, de*** garantir que les produits et services TIC certifiés selon un

l'authenticité, l'intégrité et la confidentialité de données stockées ou transmises ou traitées, ou les fonctions connexes des ***produits***, ***processus***, services et systèmes au sens du présent règlement, ou les services qu'ils offrent ou qui sont accessibles par leur intermédiaire. Il n'est pas possible d'exposer en détail dans le présent règlement les exigences de cybersécurité se rapportant à tous les produits et services TIC. Les produits et services TIC et les besoins de cybersécurité correspondants sont si diversifiés qu'il est très difficile d'établir des exigences de cybersécurité d'application universelle. Il est donc nécessaire d'adopter, aux fins de la certification, une notion large et générale de la cybersécurité, complétée par une série d'objectifs spécifiques en matière de cybersécurité qui devraient être pris en compte lors de la conception de systèmes européens de certification de cybersécurité. Les modalités selon lesquelles ces objectifs seront atteints pour des produits et services TIC spécifiques devraient ensuite être précisées en détail au niveau des différents systèmes de certification adoptés par la Commission, par exemple, en faisant référence à des normes ou à des spécifications techniques.

tel système sont conformes aux exigences spécifiées. Ces exigences concernent l'aptitude à résister, à un niveau d'assurance donné, aux actions qui visent à compromettre la disponibilité, l'authenticité, l'intégrité et la confidentialité de données stockées ou transmises ou traitées, ou les fonctions connexes des ***processus***, ***produits***, services et systèmes au sens du présent règlement, ou les services qu'ils offrent ou qui sont accessibles par leur intermédiaire. Il n'est pas possible d'exposer en détail dans le présent règlement les exigences de cybersécurité se rapportant à tous les produits et services TIC. Les produits et services TIC et les besoins de cybersécurité correspondants sont si diversifiés qu'il est très difficile d'établir des exigences de cybersécurité d'application universelle. Il est donc nécessaire d'adopter, aux fins de la certification, une notion large et générale de la cybersécurité, complétée par une série d'objectifs spécifiques en matière de cybersécurité qui devraient être pris en compte lors de la conception de systèmes européens de certification de cybersécurité. Les modalités selon lesquelles ces objectifs seront atteints pour des produits et services TIC spécifiques devraient ensuite être précisées en détail au niveau des différents systèmes de certification adoptés par la Commission, par exemple, en faisant référence à des normes ou à des spécifications techniques. ***Il est primordial que chaque système européen de certification de cybersécurité soit conçu de manière à stimuler et à encourager tous les acteurs intervenant dans le secteur concerné, afin d'élaborer et d'adopter des normes de sécurité, des normes techniques et des principes de sécurité dès la conception, à tous les stades du cycle de vie du produit ou service. Lorsque le système de certification prévoit des marques ou des labels, les conditions dans lesquelles ces marques ou labels peuvent être utilisés doivent être précisées. Ce label pouvant***

prendre la forme d'un logo numérique ou d'un code QR mentionnerait les risques liés au fonctionnement et à l'utilisation de produits et services TIC, et devrait être clair et facile à comprendre pour l'utilisateur final.

Amendement 20

Proposition de règlement
Considérant 55 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	(55 bis) Au vu de l'évolution de l'innovation, de l'accessibilité croissante des appareils connectés (IdO) et de leur nombre sans cesse plus important dans tous les secteurs de la société, il convient de prêter une attention particulière à la sécurité de tous les produits de l'IdO, même les plus simples. Par conséquent, la certification représentant un moyen essentiel pour renforcer la confiance dans le marché et accroître la sécurité et la résilience, il y aurait lieu de mettre l'accent sur les produits et services de l'IdO dans le nouveau cadre européen de certification de cybersécurité, afin de les rendre moins vulnérables et plus sûrs pour les consommateurs et les entreprises.

Amendement 21

Proposition de règlement
Considérant 56

Texte proposé par la Commission	*Amendement*
(56) ***La Commission*** devrait ***être habilitée*** à ***demander à l'ENISA de préparer des systèmes candidats pour des produits ou services TIC spécifiques.*** Sur ***la base du système candidat que propose l'ENISA***, ***la Commission devrait alors être habilitée à adopter le système européen de certification de cybersécurité*** par ***voie***	(56) ***L'ENISA*** devrait ***tenir*** à ***jour un site web spécialisé doté d'un outil en ligne facile d'utilisation reprenant les informations*** sur ***les systèmes adoptés***, ***les systèmes candidats et les systèmes demandés*** par ***la Commission***. Compte tenu de la finalité générale du présent règlement et des objectifs de sécurité qui y

d'actes d'exécution. Compte tenu de la finalité générale du présent règlement et des objectifs de sécurité qui y sont définis, tout système européen de certification de cybersécurité adopté par la Commission devrait préciser un ensemble minimal d'éléments relatifs à l'objet, au champ d'application et au fonctionnement du système considéré. Ces éléments devraient comprendre notamment le champ d'application et l'objet de la certification de cybersécurité, notamment l'indication des catégories de produits et services TIC couverts, la description détaillée des exigences de cybersécurité (par exemple par référence à des normes ou spécifications techniques), les critères et méthodes d'évaluation spécifiques, ainsi que le niveau d'assurance visé, c'est-à-dire ***élémentaire***, ***substantiel*** ou ***supérieur***.

sont définis, tout système européen de certification de cybersécurité adopté par la Commission devrait préciser un ensemble minimal d'éléments relatifs à l'objet, au champ d'application et au fonctionnement du système considéré. Ces éléments devraient comprendre notamment le champ d'application et l'objet de la certification de cybersécurité, notamment l'indication des catégories de produits et services TIC couverts, la description détaillée des exigences de cybersécurité (par exemple par référence à des normes ou spécifications techniques), les critères et méthodes d'évaluation spécifiques ***associés au fonctionnement et à l'utilisation d'un produit, processus ou service TIC et ses risques inhérents***, ainsi que le niveau d'assurance visé***: «fonctionnel»***, ***c'est-à-dire des niveaux d'assurance offrant un degré de sécurité fonctionnel, «substantiel», «élevé», ou toute combinaison de ces niveaux***. ***Ces niveaux d'assurance ne devraient pas donner à penser que la sécurité est absolue, de manière à ne pas induire l'utilisateur final en erreur. Il devrait en outre être tenu compte de tout le cycle de vie du produit. Pour préciser les risques auxquels doit pouvoir résister un produit ou un service particulier, l'ENISA devrait coordonner l'établissement d'une liste de contrôle reprenant les risques auxquels pourrait être confronté le processus, produit ou service TIC pour une catégorie donnée d'utilisateurs dans un environnement particulier.***

Amendement 22

Proposition de règlement
Considérant 56 bis (nouveau)

Texte proposé par la Commission

Amendement

(56 bis) La Commission devrait être habilitée à demander à l'ENISA de préparer des systèmes candidats pour des

produits ou services TIC spécifiques. 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 en ce qui concerne la création des systèmes européens de certification de cybersécurité pour les produits et services TIC. 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». En particulier, pour garantir 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. Lors de l'adoption de ces actes délégués, la Commission devrait fonder les systèmes de certification de cybersécurité pour les produits et service TIC sur tout système candidat pertinent proposé par l'ENISA, dans le but accroître la confiance dans le cadre de certification de cybersécurité et sa prévisibilité et y sensibiliser le public.

Amendement 23

Proposition de règlement
Considérant 56 ter (nouveau)

Texte proposé par la Commission	*Amendement*
	(56 ter) Parmi les méthodes et les procédures d'évaluation associées à chaque système européen de certification de sécurité, il conviendrait de promouvoir, au niveau de l'Union, le piratage contrôlé, dont l'objectif est d'identifier les

faiblesses et vulnérabilités des appareils et des systèmes d'information en anticipant les actions et les capacités des pirates malveillants.

Amendement 24

Proposition de règlement
Considérant 58

Texte proposé par la Commission	*Amendement*
(58) Une fois un système européen de certification de cybersécurité adopté, les fabricants de produits TIC ou les fournisseurs de services TIC devraient être en mesure de soumettre une demande de certification de leurs produits ou services à l'organisme d'évaluation de la conformité de leur choix. Les organismes d'évaluation de la conformité devraient être agréés par un organisme d'accréditation s'ils satisfont à certaines exigences précises énoncées dans le présent règlement. L'accréditation devrait être accordée pour une durée maximale de cinq ans et pouvoir être renouvelée dans les mêmes conditions pourvu que l'organisme d'évaluation de la conformité satisfasse aux exigences. Elle devrait être révoquée si les conditions de l'accréditation ne sont pas ou plus remplies ou si des mesures prises par l'organisme d'évaluation de la conformité enfreignent le présent règlement.	***(58)*** Une fois un système européen de certification de cybersécurité adopté, les fabricants de produits TIC ou les fournisseurs de services TIC devraient être en mesure de soumettre une demande de certification de leurs ***processus,*** produits ou services à l'organisme d'évaluation de la conformité de leur choix***, ou de déclarer eux-mêmes que leurs produits ou services sont conformes au système européen de certification de cybersécurité applicable*** . Les organismes d'évaluation de la conformité devraient être agréés par un organisme d'accréditation s'ils satisfont à certaines exigences précises énoncées dans le présent règlement. L'accréditation devrait être accordée pour une durée maximale de cinq ans et pouvoir être renouvelée dans les mêmes conditions pourvu que l'organisme d'évaluation de la conformité satisfasse aux exigences. Elle devrait être révoquée si les conditions de l'accréditation ne sont pas ou plus remplies ou si des mesures prises par l'organisme d'évaluation de la conformité enfreignent le présent règlement. ***En vue d'une accréditation uniforme dans l'Union européenne, les organismes nationaux d'accréditation devraient faire l'objet d'une évaluation par les pairs de leurs procédures, afin de vérifier la conformité des produits soumis à une certification de cybersécurité.***

Amendement 25

Proposition de règlement
Considérant 59

Texte proposé par la Commission	*Amendement*
(59) Il est nécessaire d'exiger que tous les États membres désignent une autorité de contrôle de la certification de cybersécurité afin de contrôler que les organismes d'évaluation de la conformité et les certificats délivrés par les organismes d'évaluation de la conformité établis sur leur territoire respectent les exigences du présent règlement et des systèmes de certification de cybersécurité pertinents. Les autorités nationales de contrôle de la certification devraient traiter les réclamations introduites par toute personne physique ou morale en rapport avec les certificats délivrés par des organismes d'évaluation de la conformité établis sur leur territoire, examiner l'objet de la réclamation dans la mesure nécessaire et informer l'auteur de la réclamation de l'état d'avancement et de l'issue de l'enquête dans un délai raisonnable. De plus, elles devraient coopérer avec les autres autorités nationales de contrôle de la certification ou d'autres autorités publiques, notamment en s'échangeant des informations sur l'éventuelle non-conformité de produits et services TIC aux exigences du présent règlement ou à celles de systèmes de certification de cybersécurité spécifiques.	(59) Il est nécessaire d'exiger que tous les États membres désignent une autorité de contrôle de la certification de cybersécurité afin de contrôler que les organismes d'évaluation de la conformité et les certificats délivrés par les organismes d'évaluation de la conformité établis sur leur territoire respectent les exigences du présent règlement et des systèmes de certification de cybersécurité pertinents. Les autorités nationales de contrôle de la certification devraient traiter les réclamations introduites par toute personne physique ou morale en rapport avec les certificats délivrés par des organismes d'évaluation de la conformité établis sur leur territoire, examiner l'objet de la réclamation dans la mesure nécessaire et informer l'auteur de la réclamation de l'état d'avancement et de l'issue de l'enquête dans un délai raisonnable. De plus, elles devraient coopérer avec les autres autorités nationales de contrôle de la certification ou d'autres autorités publiques, notamment en s'échangeant des informations sur l'éventuelle non-conformité de produits et services TIC aux exigences du présent règlement ou à celles de systèmes de certification de cybersécurité spécifiques. ***Elles devraient en outre superviser et contrôler la conformité des autodéclarations de conformité et s'assurer que les certificats européens de cybersécurité ont été délivrés par des organismes d'évaluation de la conformité dans le respect des exigences énoncées dans le présent règlement, notamment des règles adoptées par le groupe européen de certification de cybersécurité et des exigences énoncées dans le système européen de certification de cybersécurité correspondant. Une***

coopération efficace entre les autorités nationales de contrôle de la certification est indispensable à la mise en œuvre correcte des systèmes européens de certification de cybersécurité et des questions techniques en ce qui concerne la cybersécurité des produits et services TIC. La Commission devrait faciliter l'échange d'informations grâce à la mise à disposition d'un système général de soutien à l'information électronique, par exemple, le système d'information et de communication pour la surveillance des marchés (ICSMS) et le système européen d'alerte rapide pour les produits dangereux (RAPEX) déjà utilisés par les autorités de surveillance du marché conformément au règlement (CE) nº 765/2008.

Amendement 26

Proposition de règlement
Considérant 63

Texte proposé par la Commission	*Amendement*
(63) Afin de préciser les critères d'accréditation des organismes d'évaluation de la conformité, le pouvoir d'adopter des actes conformément à l'article 290 du traité sur le fonctionnement de l'Union européenne devrait être délégué à la Commission. Il convient que la Commission procède aux consultations appropriées durant son travail préparatoire, y compris au niveau des experts. Ces consultations devraient être menées conformément aux principes définis dans l'accord interinstitutionnel «Mieux légiférer» du 13 avril 2016. En particulier, pour assurer leur égale participation à la préparation des actes délégués, le Parlement européen et le Conseil devraient recevoir tous les documents au même moment que les experts des États membres, et leurs experts avoir systématiquement accès aux réunions des groupes d'experts de la	***supprimé***

Commission traitant de la préparation des actes délégués.

Amendement 27

Proposition de règlement
Considérant 65

Texte proposé par la Commission	*Amendement*
(65) La procédure d'examen devrait être utilisée pour l'adoption d'actes d'exécution concernant les systèmes européens de certification de cybersécurité applicables à des produits et services TIC; concernant les modalités d'exécution des enquêtes menées par l'Agence; et concernant les circonstances, les formats et les procédures de notification à la Commission, par les autorités nationales de contrôle de la certification, des organismes d'évaluation de la conformité accrédités.	(65) La procédure d'examen devrait être utilisée pour l'adoption d'actes d'exécution concernant les systèmes européens de certification de cybersécurité applicables à des ***processus,*** produits et services TIC; concernant les modalités d'exécution des enquêtes menées par l'Agence; et concernant les circonstances, les formats et les procédures de notification à la Commission, par les autorités nationales de contrôle de la certification, des organismes d'évaluation de la conformité accrédités***, compte tenu de l'efficacité avérée de l'outil de notification électronique «organismes "nouvelle approche" notifiés et désignés» (NANDO)***.

Amendement 28

Proposition de règlement
Considérant 66

Texte proposé par la Commission	*Amendement*
(66) Le fonctionnement de l'Agence devrait faire l'objet d'une évaluation indépendante. Cette évaluation devrait ***s'intéresser à*** la ***réalisation*** des objectifs, ***aux*** méthodes de travail et ***à*** la pertinence ***des missions*** de ***l'Agence***. L'évaluation devrait également porter sur l'impact, l'efficacité et l'efficience du cadre européen de certification de cybersécurité.	(66) Le fonctionnement de l'Agence devrait faire l'objet d'une évaluation indépendante. Cette évaluation devrait ***se pencher sur*** la ***régularité et l'adéquation*** des ***crédits engagés par l'Agence pour atteindre ses*** objectifs, ***et comporter une description de ses*** méthodes de travail et ***de*** la pertinence de ***ses missions***. L'évaluation devrait également porter sur l'impact, l'efficacité et l'efficience du cadre européen de certification de cybersécurité.

Amendement 29

Proposition de règlement
Article 2 – alinéa 1 – point 11

Texte proposé par la Commission	*Amendement*
(11) ***«produit ou*** service ***TIC»***, ***tout élément*** ou ***groupe d'éléments*** appartenant aux réseaux et systèmes d'information;	(11) ***«processus, produit et service TIC», un produit,*** service***, processus***, ***système*** ou ***une combinaison de ceux-ci qui est un élément*** appartenant aux réseaux et systèmes d'information; *(Cette modification s'applique à l'ensemble du texte législatif à l'examen;. son adoption impose des adaptations techniques dans tout le texte.)*

Amendement 30

Proposition de règlement
Article 2 – alinéa 1 – point 11 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	(11 bis) «autorité nationale de contrôle de la certification», une autorité d'un État membre chargée des fonctions de suivi, d'exécution et de contrôle liées à la certification de cybersécurité sur son territoire;

Amendement 31

Proposition de règlement
Article 2 – alinéa 1 – point 16 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	(16 bis) «autodéclaration de conformité», la déclaration d'un fabricant certifiant que son processus, produit ou service TIC est conforme aux systèmes européens de certification de cybersécurité mentionnés.

Amendement 32

Proposition de règlement
Article 3 – paragraphe 1

Texte proposé par la Commission	*Amendement*
1. L'Agence exécute les missions qui lui sont assignées par le présent règlement dans le but de contribuer à ***assurer*** un niveau élevé de cybersécurité ***dans*** l'Union.	1. L'Agence exécute les missions qui lui sont assignées par le présent règlement dans le but de contribuer à ***obtenir*** un niveau ***commun*** élevé de cybersécurité, ***afin de prévenir les cyberattaques au sein de*** l'Union ***et réduire ainsi la fragmentation du marché intérieur et d'améliorer son fonctionnement***.

Amendement 33

Proposition de règlement
Article 4 – paragraphe 5

Texte proposé par la Commission	*Amendement*
5. L'Agence ***accroît*** les capacités dans le domaine de la cybersécurité au niveau de l'Union afin de compléter l'action des États membres en matière de prévention des cybermenaces et de réaction à celles-ci, notamment en cas d'incidents transfrontières.	5. L'Agence ***contribue à accroître*** les capacités dans le domaine de la cybersécurité au niveau de l'Union afin de compléter ***et de renforcer*** l'action des États membres en matière de prévention des cybermenaces et de réaction à celles-ci, notamment en cas d'incidents transfrontières.

Amendement 34

Proposition de règlement
Article 4 – paragraphe 6

Texte proposé par la Commission	*Amendement*
6. L'Agence promeut le recours à la certification***, notamment*** en ***contribuant*** à l'établissement et au maintien d'un cadre de certification de cybersécurité au niveau de l'Union, conformément ***au titre III du présent règlement***, en vue de rendre plus transparente l'assurance de la cybersécurité des produits et services TIC et, partant, de	6. L'Agence promeut le recours à la certification ***tout*** en ***évitant la fragmentation due au manque de coordination entre les systèmes de certification existants de l'Union. L'Agence contribue*** à l'établissement et au maintien d'un cadre de certification de cybersécurité au niveau de l'Union,

rehausser la confiance dans le marché ***intérieur*** numérique.	conformément ***aux articles 43 à 54 [***titre III***]***, en vue de rendre plus transparente l'assurance de la cybersécurité des produits et services TIC et, partant, de rehausser la confiance dans le marché ***unique*** numérique.

Amendement 35

Proposition de règlement
Article 1 – paragraphe 7

Texte proposé par la Commission	*Amendement*
7. L'Agence promeut un niveau élevé de sensibilisation des particuliers et des entreprises aux questions liées à la cybersécurité.	7. L'Agence promeut un niveau élevé de sensibilisation des particuliers***, des autorités*** et des entreprises aux questions liées à la cybersécurité.

Amendement 36

Proposition de règlement
Article 5 – alinéa 1 – point 1

Texte proposé par la Commission	*Amendement*
1. en apportant son concours et ses conseils***, en particulier sous la forme d'avis indépendants et de travaux préparatoires,*** concernant l'élaboration et la révision de la politique et du droit de l'Union dans le domaine de la cybersécurité, ainsi que les initiatives politiques et législatives sectorielles mettant en jeu des questions liées à la cybersécurité;	1. en apportant son concours et ses conseils concernant l'élaboration et la révision de la politique et du droit de l'Union dans le domaine de la cybersécurité, ainsi que les initiatives politiques et législatives sectorielles mettant en jeu des questions liées à la cybersécurité;

Justification

L'Agence devrait avoir toute discrétion quant aux moyens qu'elle utilise pour exécuter ses tâches.

Amendement 37

Proposition de règlement

Article 5 – alinéa 1 – point 2 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	***2 bis. en aidant le comité européen de la protection des données institué par le règlement (UE) 2016/679 à élaborer des lignes directrices afin de préciser, sur le plan technique, les conditions permettant l'utilisation licite des données à caractère personnel par les responsables du traitement des données aux fins de la sécurité informatique, en vue de protéger leurs infrastructures en détectant et en bloquant les attaques contre leurs systèmes d'information, dans le cadre: i) du règlement (UE) 2016/679[1 bis]; ii) de la directive (UE) 2016/1148[1 ter]; et iii) de la directive 2002/58/CE[1 quater];* [1 bis] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), JO L 119 du 4.5.2016, p. 1. [1 ter] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (JO L 119 du 4.5.2016, p. 1). [1 quater] Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union (JO L 194 du 19.7.2016, p. 1).

Justification

Établissement de mécanismes de coopération appropriés.

Amendement 38

Proposition de règlement
Article 5 – alinéa 1 – point 4 – sous-point 2

Texte proposé par la Commission	*Amendement*
(2) l'amélioration du niveau de sécurité des communications électroniques, y compris en fournissant une expertise et des conseils, ainsi qu'en facilitant l'échange de bonnes pratiques entre les autorités compétentes;	(2) l'amélioration du niveau de sécurité des communications électroniques, ***du stockage et du traitement des données,*** y compris en fournissant une expertise et des conseils, ainsi qu'en facilitant l'échange de bonnes pratiques entre les autorités compétentes;

Amendement 39

Proposition de règlement
Article 6 – paragraphe 2 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	2 bis. L'Agence facilite la mise en place et le lancement d'un projet européen à long terme sur la cybersécurité afin de soutenir le développement d'une industrie de la cybersécurité indépendante de l'Union et d'intégrer la cybersécurité dans toutes les évolutions en matière de TIC au niveau de l'Union.

Justification

L'ENISA devrait conseiller les législateurs en matière d'élaboration des politiques afin de permettre à l'Union de rattraper les industries de sécurité informatique des pays tiers. Le projet devrait être comparable, par son ampleur, à ce qui a déjà été réalisé dans le secteur de l'aviation (voir l'exemple d'Airbus). Cette démarche est nécessaire pour mettre au point une industrie européenne des TIC forte, souveraine et fiable (voir l'étude de l'unité de prospective scientifique (STOA) PE 614.531).

Amendement 40

Proposition de règlement
Article 7 – paragraphe 5 – alinéa 1

Texte proposé par la Commission	*Amendement*
À la demande d'au moins ***deux États membres concernés*** et dans le seul but de fournir des conseils sur la prévention des incidents, l'Agence apporte son concours ou procède elle-même à une enquête technique ex post à la suite de la notification, par les entreprises exposées, d'incidents ayant un impact important ou significatif conformément à la directive (UE) 2016/1148. L'Agence procède également à une enquête de ce type à la demande dûment justifiée de la Commission, en accord avec les États membres concernés, lorsque les incidents atteignent plus de deux États membres.	À la demande d'au moins ***un État membre concerné*** et dans le seul but de fournir des conseils sur la prévention des incidents, l'Agence apporte son concours ou procède elle-même à une enquête technique ex post à la suite de la notification, par les entreprises exposées, d'incidents ayant un impact important ou significatif conformément à la directive (UE) 2016/1148. L'Agence procède également à une enquête de ce type à la demande dûment justifiée de la Commission, en accord avec les États membres concernés, lorsque les incidents atteignent plus de deux États membres.

Amendement 41

Proposition de règlement
Article 7 – paragraphe 8 – point a

Texte proposé par la Commission	*Amendement*
(a) agrégeant des rapports provenant de sources nationales en vue de contribuer à former une appréciation commune de la situation;	(a) agrégeant des rapports provenant de sources nationales ***et internationales*** en vue de contribuer à former une appréciation commune de la situation;

Amendement 42

Proposition de règlement
Article 8 – alinéa 1 – point a – sous-point 1 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	(1 bis) procède, en coopération avec le groupe européen de certification de cybersécurité, aux évaluations des procédures pour la délivrance des certificats européens de cybersécurité mises en place par les organismes d'évaluation de la conformité visés à

l'article 51, en vue d'assurer une application uniforme du présent règlement par les organismes d'évaluation de la conformité lorsqu'ils délivrent des certificats;

Amendement 43

Proposition de règlement
Article 8 – alinéa 1 – point a – sous-point 1 ter (nouveau)

Texte proposé par la Commission	*Amendement*
	(1 ter) réalisant des contrôles réguliers indépendants ex post de la conformité de produits et services TIC certifiés par les systèmes européens de certification de cybersécurité;

Amendement 44

Proposition de règlement
Article 8 – alinéa 1 – point a – sous-point 3

Texte proposé par la Commission	*Amendement*
(3) établissant et publiant des lignes directrices, ainsi qu'en mettant au point des bonnes pratiques en ce qui concerne les exigences de cybersécurité de produits et services TIC, en coopération avec les autorités nationales de contrôle de la certification et l'industrie;	(3) établissant et publiant des lignes directrices, ainsi qu'en mettant au point des bonnes pratiques***, y compris sur les principes d'hygiène cybernétique et les moyens de contrer les portes dérobées secrètes,*** en ce qui concerne les exigences de cybersécurité de produits et services TIC, en coopération avec les autorités nationales de contrôle de la certification et le secteur ***dans le cadre d'un processus formel, normalisé et transparent***;

Amendement 45

Proposition de règlement
Article 8 – alinéa 1 – point b

Texte proposé par la Commission	*Amendement*
(b) ***facilite*** l'établissement et l'adoption de normes européennes et internationales en matière de gestion des risques et de sécurité des produits et services TIC***;*** formule, en collaboration avec les États membres, des avis et des lignes directrices concernant les domaines techniques liés aux exigences de sécurité qui s'imposent aux opérateurs de services essentiels et aux fournisseurs de service numérique, et concernant les normes existantes, y compris les normes nationales des États membres, en application de l'article 19, paragraphe 2, de la directive (UE) 2016/1148;	(b) ***consulte les organisations internationales et européennes de normalisation sur l'élaboration de normes, afin de veiller à l'adéquation des normes utilisées dans les systèmes européens de certification de cybersécurité et facilite*** l'établissement et l'adoption de normes européennes et internationales ***pertinentes*** en matière de gestion des risques et de sécurité des produits et services TIC***, et*** formule, en collaboration avec les États membres, des avis et des lignes directrices concernant les domaines techniques liés aux exigences de sécurité qui s'imposent aux opérateurs de services essentiels et aux fournisseurs de service numérique, et concernant les normes existantes, y compris les normes nationales des États membres, en application de l'article 19, paragraphe 2, de la directive (UE) 2016/1148;

Amendement 46

Proposition de règlement
Article 8 – alinéa 1 – point b bis (nouveau)

Texte proposé par la Commission	*Amendement*
	(b bis) élaborer des lignes directrices précisant comment, et à quel moment, les États membres doivent s'informer mutuellement lorsqu'ils ont connaissance d'une vulnérabilité qui n'est pas publiquement connue dans un processus, produit ou service TIC certifié conformément au titre III du présent règlement, y compris des lignes directrices sur la coordination des politiques de divulgation des vulnérabilités.

Amendement 47

Proposition de règlement
Article 8 – alinéa 1 – point b ter (nouveau)

Texte proposé par la Commission	*Amendement*
	(b ter) élaborer des lignes directrices relatives aux exigences de sécurité minimales pour les équipements informatiques mis sur le marché dans l'Union ou exportés à partir de l'Union.

Amendement 48

Proposition de règlement
Article 9 – alinéa 1 – point d

Texte proposé par la Commission	*Amendement*
(d) regroupe, organise et met à la disposition du public, par l'intermédiaire d'un portail spécialisé, des informations sur la cybersécurité, fournies par les institutions, organes et organismes de l'Union;	(d) regroupe, organise et met à la disposition du public, par l'intermédiaire d'un portail spécialisé, des informations sur la cybersécurité***, notamment des informations sur les incidents importants en matière de cybersécurité et les violations majeures de données***, fournies par les institutions, organes et organismes de l'Union;

Amendement 49

Proposition de règlement
Article 9 – alinéa 1 – point e

Texte proposé par la Commission	*Amendement*
(e) sensibilise le public sur les risques liés à la cybersécurité et fournit, à l'intention des ***particuliers*** et des organisations, des orientations sur les bonnes pratiques à adopter par les utilisateurs***;***	(e) sensibilise le public sur les risques liés à la cybersécurité et fournit, à l'intention des ***citoyens*** et des organisations, des orientations sur les bonnes pratiques à adopter par les utilisateurs ***et encourage l'adoption de mesures préventives vigoureuses en matière de sécurité informatique et une protection fiable des données et du respect de la vie privée.***

Amendement 50

Proposition de règlement
Article 9 – alinéa 1 – point g bis (nouveau)

Texte proposé par la Commission	*Amendement*
	(g bis) encourage une coopération plus étroite et l'échange de bonnes pratiques entre les États membres en matière d'éducation, d'hygiène cybernétique et de sensibilisation dans le domaine de la cybersécurité

Amendement 51

Proposition de règlement
Article 10 – alinéa 1 – point a

Texte proposé par la Commission	*Amendement*
(a) ***conseille*** l'Union et les États membres sur les besoins et les priorités en matière de recherche dans le domaine de la cybersécurité, afin que des réponses efficaces puissent être apportées face aux risques et aux menaces actuels et émergents, y compris en ce qui concerne les technologies de l'information et de la communication nouvelles et émergentes, et afin que les technologies de prévention des risques soient utilisées d'une manière efficace;	(a) ***assure la consultation préalable des groupes d'utilisateurs concernés et conseille*** l'Union et les États membres sur les besoins et les priorités en matière de recherche dans le domaine de la cybersécurité, afin que des réponses efficaces puissent être apportées face aux risques et aux menaces actuels et émergents, y compris en ce qui concerne les technologies de l'information et de la communication nouvelles et émergentes, et afin que les technologies de prévention des risques soient utilisées d'une manière efficace;

Amendement 52

Proposition de règlement
Article 13 – paragraphe 1

Texte proposé par la Commission	*Amendement*
1. Le conseil d'administration est composé d'un représentant de chaque État membre, et de deux représentants nommés par la Commission. Tous les représentants	1. Le conseil d'administration est composé d'un représentant de chaque État membre, et de deux représentants nommés par la Commission ***et le Parlement européen***. Tous les représentants disposent

disposent du droit de vote.	du droit de vote.

Amendement 53

Proposition de règlement
Article 14 – paragraphe 1 – point e

Texte proposé par la Commission	*Amendement*
(e) évalue et adopte le rapport annuel consolidé sur les activités de l'Agence et transmet, au plus tard le 1er juillet de l'année suivante, le rapport et son évaluation au Parlement européen, au Conseil, à la Commission et à la Cour des comptes. Le rapport annuel inclut les comptes et ***décrit*** la manière dont l'Agence atteint ses indicateurs de performance. Le rapport annuel est rendu public;	(e) évalue et adopte le rapport annuel consolidé sur les activités de l'Agence et transmet, au plus tard le 1er juillet de l'année suivante, le rapport et son évaluation au Parlement européen, au Conseil, à la Commission et à la Cour des comptes. Le rapport annuel inclut les comptes***, décrit l'adéquation des crédits engagés*** et ***évalue*** la manière dont l'Agence ***a été efficace et a*** atteint ses indicateurs de performance. Le rapport annuel est rendu public;

Amendement 54

Proposition de règlement
Article 14 – paragraphe 1 – point m

Texte proposé par la Commission	*Amendement*
(m) nomme le directeur exécutif et, le cas échéant, prolonge son mandat ou le démet de ses fonctions conformément à l'article 33 du présent règlement;	(m) nomme le directeur exécutif ***à l'issue d'une sélection fondée sur des critères professionnels*** et, le cas échéant, prolonge son mandat ou le démet de ses fonctions conformément à l'article 33 du présent règlement;

Amendement 55

Proposition de règlement
Article 14 – paragraphe 1 – point o

Texte proposé par la Commission	*Amendement*
(o) prend toutes les décisions relatives à la mise en place des structures internes de l'Agence et, le cas échéant, à leur modification, en tenant compte des besoins	(o) prend toutes les décisions relatives à la mise en place des structures internes de l'Agence et, le cas échéant, à leur modification, en tenant compte des besoins

liés à l'activité de l'Agence et en respectant le principe d'une gestion budgétaire saine;

liés à l'activité de l'Agence ***telle que décrite dans le présent règlement*** et en respectant le principe d'une gestion budgétaire saine;

Amendement 56

Proposition de règlement
Article 19 – paragraphe 2

Texte proposé par la Commission	*Amendement*
2. Le directeur exécutif fait rapport au Parlement européen sur l'exécution de ses tâches, lorsqu'il y est invité. Le Conseil peut inviter le directeur exécutif à lui faire rapport sur l'exécution de ses tâches.	2. Le directeur exécutif fait rapport au Parlement européen sur l'exécution de ses tâches, ***chaque année ou*** lorsqu'il y est invité. Le Conseil peut inviter le directeur exécutif à lui faire rapport sur l'exécution de ses tâches.

Amendement 57

Proposition de règlement
Article 20 – paragraphe 1

Texte proposé par la Commission	*Amendement*
1. Le conseil d'administration crée, sur proposition du directeur exécutif, un groupe permanent des parties prenantes composé d'experts reconnus représentant les parties prenantes concernées, comme les entreprises du secteur des TIC, les fournisseurs de réseaux de communications électroniques ou de services accessibles au public, les organisations de consommateurs, les experts universitaires en ***matière*** de ***cybersécurité*** et les représentants des autorités compétentes notifiées au titre de la [directive établissant le code des communications électroniques européen], ainsi que les autorités chargées du respect de la loi et de la protection des données.	1. Le conseil d'administration crée, sur proposition du directeur exécutif, un groupe permanent des parties prenantes composé d'experts reconnus représentant les parties prenantes concernées, comme les entreprises du secteur des TIC, ***et*** les fournisseurs de réseaux de communications électroniques ou de services accessibles au public, ***notamment le secteur des TIC et les fournisseurs, les associations de petites et moyennes entreprises,*** les organisations ***et les associations*** de consommateurs, les experts universitaires ***spécialisés*** en ***cybersécurité, dans l'Union, de même que les organisations européennes*** de ***normalisation telles que définies à l'article 2, paragraphe 8, du règlement (UE) nº 1025/2012, les agences et organes sectoriels pertinents de l'Union*** et les représentants des autorités compétentes notifiées au titre de la [directive établissant

le code des communications électroniques européen], ainsi que les autorités chargées du respect de la loi et de la protection des données.

Amendement 58

Proposition de règlement
Article 20 – paragraphe 4

Texte proposé par la Commission	*Amendement*
4. La durée du mandat des membres du groupe permanent des parties prenantes est de deux ans et demi. Les membres du conseil d'administration ne peuvent pas être membres du groupe permanent des parties prenantes. Des experts de la Commission et des États membres sont autorisés à assister aux réunions et à prendre part aux travaux du groupe permanent des parties prenantes. Des représentants d'autres organismes jugés intéressants par le directeur exécutif, qui ne sont pas membres du groupe permanent des parties prenantes, peuvent être invités à assister aux réunions du groupe permanent des parties prenantes et à prendre part à ses travaux.	***4.*** La durée du mandat des membres du groupe permanent des parties prenantes est de deux ans et demi. Les membres du conseil d'administration ***et du conseil exécutif, à l'exception du directeur exécutif,*** ne peuvent pas être membres du groupe permanent des parties prenantes. Des experts de la Commission et des États membres sont autorisés à assister aux réunions et à prendre part aux travaux du groupe permanent des parties prenantes. Des représentants d'autres organismes jugés intéressants par le directeur exécutif, qui ne sont pas membres du groupe permanent des parties prenantes, peuvent être invités à assister aux réunions du groupe permanent des parties prenantes et à prendre part à ses travaux.

Amendement 59

Proposition de règlement
Article 20 – paragraphe 5

Texte proposé par la Commission	*Amendement*
5. Le groupe permanent des parties prenantes conseille l'Agence dans l'exercice de ses activités. Il conseille en particulier le directeur exécutif lors de l'élaboration d'une proposition de programme de travail pour l'Agence ainsi que pour la communication avec les parties prenantes concernées sur toutes les	5. Le groupe permanent des parties prenantes conseille l'Agence dans l'exercice de ses activités. Il conseille en particulier le directeur exécutif lors de l'élaboration d'une proposition de programme de travail pour l'Agence ainsi que pour la communication avec les parties prenantes concernées sur toutes les

questions liées au programme de travail.	questions liées au programme de travail. ***Il peut également proposer à la Commission de demander à l'Agence d'élaborer des systèmes européens de certification de cybersécurité candidats conformément à l'article 44, à son initiative ou dans le sillage de propositions émanant de parties prenantes concernées.***

Amendement 60

Proposition de règlement
Article 20 – paragraphe 5 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	5 bis. Le groupe permanent des parties prenantes conseille l'Agence dans le cadre de l'élaboration de systèmes européens de certification de cybersécurité candidats.

Amendement 61

Proposition de règlement
Article 23 – paragraphe 2

Texte proposé par la Commission	*Amendement*
2. L'Agence veille à ce que le public et toute partie intéressée reçoivent une information appropriée, objective, fiable et facilement accessible, notamment en ce qui concerne le résultat de ses travaux. Elle rend également publiques les déclarations d'intérêt faites conformément à l'article 22.	2. L'Agence veille à ce que le public et toute partie intéressée reçoivent une information appropriée, objective, fiable et facilement accessible, notamment en ce qui concerne ***les débats et*** le résultat de ses travaux. Elle rend également publiques les déclarations d'intérêt faites conformément à l'article 22.

Justification

La transparence doit être respectée, compte tenu de l'application de l'article 24.

Amendement 62

Proposition de règlement

Article 43 – alinéa 1

Texte proposé par la Commission	*Amendement*
Un système européen de certification de cybersécurité atteste que les produits et services TIC qui ont été certifiés conformément à ce système satisfont à des exigences spécifiées concernant leur capacité à résister, à un niveau d'assurance donné, à des actions visant à compromettre la disponibilité, l'authenticité, l'intégrité ou la confidentialité des données stockées, transmises ou traitées ou des fonctions ou services associés qui sont offerts ou accessibles par ces ***produits***, ***processus***, services et systèmes.	Un système européen de certification de cybersécurité ***est établi afin de renforcer le niveau de sécurité au sein du marché unique numérique et d'adopter une approche harmonisée, au niveau de l'Union, de la certification européenne dans l'optique de veiller à la résistance des produits, services et systèmes TIC aux cyberattaques.*** ***Il*** atteste que les ***processus,*** produits et services TIC qui ont été certifiés conformément à ce système satisfont à des exigences ***et propriétés communes*** spécifiées concernant leur capacité à résister, à un niveau d'assurance donné, à des actions visant à compromettre la disponibilité, l'authenticité, l'intégrité ou la confidentialité des données stockées, transmises ou traitées ou des fonctions ou services associés qui sont offerts ou accessibles par ces ***processus***, ***produits***, services et systèmes.

Amendement 63

Proposition de règlement
Article 43 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	Article 43 bis ***Programme de travail*** ***L'ENISA établit, après consultation du groupe européen de certification de cybersécurité et du groupe permanent des parties prenantes et après approbation de la Commission, un programme de travail précisant les actions communes à entreprendre au niveau de l'Union pour assurer une application cohérente du présent titre et contenant une liste prioritaire des produits et services TIC devant, selon elle, être soumis à un***

système européen de certification de cybersécurité.

Ce programme de travail est établi au plus tard [six mois après l'entrée en vigueur du présent règlement] et un nouveau programme de travail est ensuite établi tous les deux ans. Le programme de travail annuel est rendu public.

Amendement 64

Proposition de règlement
Article 44 – paragraphe 1

Texte proposé par la Commission	*Amendement*
1. À la suite d'une demande de la Commission, l'ENISA élabore un système européen de certification de cybersécurité candidat qui satisfait aux exigences énoncées aux articles 45, 46 et 47 du présent règlement. Les États membres ou le groupe européen de certification de cybersécurité (le «groupe») établi en vertu de l'article 53 peuvent proposer à la Commission l'élaboration d'un système européen de certification de cybersécurité candidat.	1. À la suite d'une demande de la Commission, l'ENISA élabore un système européen de certification de cybersécurité candidat qui satisfait aux exigences énoncées aux articles 45, 46 et 47 du présent règlement. Les États membres ou le groupe européen de certification de cybersécurité (le «groupe») établi en vertu de l'article 53 ***ou le groupe permanent des parties prenantes établi conformément à l'article 20*** peuvent proposer à la Commission l'élaboration d'un système européen de certification de cybersécurité candidat.

Amendement 65

Proposition de règlement
Article 44 – paragraphe 2

Texte proposé par la Commission	*Amendement*
2. Lors de l'élaboration des systèmes candidats visés au paragraphe 1, l'ENISA consulte ***toutes les*** parties prenantes ***concernées et travaille en étroite collaboration avec le groupe. Celui-ci fournit à l'ENISA l'aide et l'expertise dont elle a besoin*** dans le cadre ***de l'élaboration du système candidat***, ***notamment*** en ***formulant*** des ***avis si***	2. Lors de l'élaboration des systèmes candidats visés au paragraphe 1, l'ENISA consulte ***le groupe permanent des*** parties prenantes***, notamment les organisations européennes de normalisation, ainsi que toutes les autres parties prenantes concernées, y compris les associations de consommateurs,*** dans le cadre ***d'une procédure formelle, normalisée et***

nécessaire.	***transparente***, ***et travaille*** en ***étroite collaboration avec le groupe en tenant compte*** des ***normes nationales et internationales déjà existantes***. ***Lors de l'élaboration de chaque système candidat, l'ENISA établit une liste de contrôle des risques et des caractéristiques correspondantes de cybersécurité.*** ***Celui-ci fournit à l'ENISA l'aide et l'expertise dont elle a besoin dans le cadre de l'élaboration du système candidat, notamment en formulant des avis si nécessaire.*** ***Le cas échéant, l'ENISA peut également mettre en place un groupe d'experts pour la consultation des parties prenantes composé de membres du groupe permanent des parties prenantes et de toute autre partie prenante possédant des compétences particulières dans le domaine d'un système candidat donné, afin d'apporter une aide et des conseils supplémentaires.***

Amendement 66

Proposition de règlement
Article 44 – paragraphe 3

Texte proposé par la Commission	*Amendement*
3. L'Agence transmet à la Commission le système européen de certification de cybersécurité candidat élaboré conformément au paragraphe 2.	3. L'Agence transmet à la Commission le système européen de certification de cybersécurité candidat élaboré conformément au paragraphe 2***; la Commission évalue alors la capacité de ce système à réaliser les objectifs de la demande visée au paragraphe 1***.

Amendement 67

Proposition de règlement
Article 44 – paragraphe 3 bis (nouveau)

Texte proposé par la Commission	*Amendement*

3 bis. L'ENISA respecte le secret professionnel en ce qui concerne toutes les informations obtenues dans l'accomplissement de ses missions au titre du présent règlement.

Amendement 68

Proposition de règlement
Article 44 – paragraphe 4

Texte proposé par la Commission	*Amendement*
4. La Commission***, se fondant sur le système candidat proposé par l'ENISA, peut*** adopter des actes ***d'exécution***, conformément à l'article ***55***, ***paragraphe 1, prévoyant des*** systèmes européens de certification de cybersécurité pour les produits et services TIC qui satisfont aux exigences des articles 45, 46 et 47 du présent règlement.	4. La Commission ***est habilitée à*** adopter des actes ***délégués***, conformément à l'article ***55 bis***, ***en ce qui concerne l'établissement de*** systèmes européens de certification de cybersécurité pour les produits et services TIC qui satisfont aux exigences des articles 45, 46 et 47 du présent règlement. ***Lors de l'adoption de ces actes délégués, la Commission fonde les systèmes de certification de cybersécurité pour les produits et service TIC sur tout système candidat pertinent proposé par l'ENISA. La Commission peut consulter le comité européen de la protection des données et tenir compte de sa position avant d'adopter ces actes délégués.***

Amendement 69

Proposition de règlement
Article 44 – paragraphe 5

Texte proposé par la Commission	*Amendement*
5. L'ENISA tient à jour un site web spécifique fournissant des informations sur les systèmes européens de certification de cybersécurité et leur assurant une publicité.	5. L'ENISA tient à jour un site web spécifique fournissant des informations sur les systèmes européens de certification de cybersécurité et leur assurant une publicité***, notamment les informations sur tous les systèmes candidats dont la Commission a demandé l'élaboration à l'ENISA***.

Amendement 70

Proposition de règlement
Article 45 – alinéa 1 – partie introductive

Texte proposé par la Commission	*Amendement*
Un système européen de certification de cybersécurité est conçu de façon à prendre en compte***, le cas échéant,*** les objectifs de sécurité suivants:	***Chaque*** système européen de certification de cybersécurité est conçu de façon à prendre en compte ***au moins*** les objectifs de sécurité suivants***, dans la mesure où ils sont pertinents***:

Amendement 71

Proposition de règlement
Article 45 – alinéa 1 – point g

Texte proposé par la Commission	*Amendement*
(g) veiller à ce que les produits et services TIC soient dotés de logiciels à jour et sans vulnérabilités connues***,*** et de mécanismes permettant d'assurer les mises à jour des logiciels en toute sécurité.	(g) veiller à ce que les produits et services TIC soient dotés de logiciels ***et des équipements*** à jour et sans vulnérabilités connues***; veiller à ce qu'ils soient conçus et mis en œuvre de manière à réellement limiter leur propension aux vulnérabilités*** et ***dotés*** de mécanismes permettant d'assurer les mises à jour des logiciels en toute sécurité***, notamment en ce qui concerne les mises à niveau des équipements et les mises à jour de sécurité automatiques***.

Amendement 72

Proposition de règlement
Article 45 – alinéa 1 – point g bis (nouveau)

Texte proposé par la Commission	*Amendement*
	(g bis) veiller à ce que les produits et services TIC soient développés et exploités de sorte qu'un niveau élevé de cybersécurité et de protection des données soit préconfiguré, conformément au principe de la «sécurité dès la

conception».

Amendement 73

Proposition de règlement
Article 46 – paragraphe 1

Texte proposé par la Commission	*Amendement*
1. ***Un*** système européen de certification de cybersécurité peut préciser un ou plusieurs des niveaux d'assurance suivants: ***élémentaire***, ***substantiel et/***ou ***élevé***, pour les produits et services TIC certifiés dans le cadre de ce système.	1. ***Chaque*** système européen de certification de cybersécurité peut préciser un ou plusieurs des niveaux d'assurance ***fondée sur le risque*** suivants: ***«fonctionnel»***, ***«substantiel»*** et ***«élevé»***, pour les produits et services TIC certifiés dans le cadre de ce système. ***Les niveaux d'assurance fondée sur le risque de chaque système européen de certification de cybersécurité candidat sont identifiés sur la base des risques visés sur la liste de contrôle établie à l'article 44, paragraphe 2, et de la présence de caractéristiques de cybersécurité pour contrer ces risques dans les produits et services TIC auxquels le système de certification s'applique.***

Amendement 74

Proposition de règlement
Article 46 – paragraphe 1 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	1 bis. Chaque système indique la méthode ou la procédure d'évaluation à suivre pour délivrer des certificats à chaque niveau d'assurance, en fonction de l'utilisation prévue et du risque inhérent aux produits et services TIC dans le cadre de ce système.

Amendement 75

Proposition de règlement
Article 46 – paragraphe 2 – partie introductive

Texte proposé par la Commission	*Amendement*
2. Les niveaux d'assurance ***élémentaire***, ***substantiel*** et ***élevé*** satisfont respectivement aux critères suivants:	2. Les niveaux d'assurance ***«fonctionnel»***, ***«substantiel»*** et ***«élevé»*** satisfont respectivement aux critères suivants:

Amendement 76

Proposition de règlement
Article 46 – paragraphe 2 – point a

Texte proposé par la Commission	*Amendement*
(a) le niveau d'assurance ***élémentaire*** renvoie à un certificat délivré dans le cadre d'un système européen de certification de cybersécurité qui accorde un degré ***limité*** de fiabilité aux qualités de cybersécurité revendiquées ou prétendues d'un produit ou ***d'un*** service TIC, et caractérisé sur la base de spécifications techniques, normes et procédures y afférents, y compris les contrôles techniques, dont l'objectif est de réduire le risque d'incidents de cybersécurité;	(a) le niveau d'assurance ***«fonctionnel»*** renvoie à un certificat délivré dans le cadre d'un système européen de certification de cybersécurité qui accorde un degré ***approprié*** de fiabilité aux qualités de cybersécurité revendiquées ou prétendues d'un ***processus,*** produit ou service TIC, et caractérisé sur la base de spécifications techniques, normes et procédures y afférents, y compris les contrôles techniques, dont l'objectif est de réduire le risque d'incidents de cybersécurité;

Amendement 77

Proposition de règlement
Article 46 – paragraphe 2 – point b

Texte proposé par la Commission	*Amendement*
(b) le niveau d'assurance ***substantiel*** renvoie à un certificat délivré dans le cadre d'un système européen de certification de cybersécurité qui accorde un degré substantiel de fiabilité aux qualités de cybersécurité revendiquées ou prétendues d'un produit ou ***d'un*** service TIC, et caractérisé sur la base de spécifications techniques, normes et procédures y	(b) le niveau d'assurance ***«substantiel»*** renvoie à un certificat délivré dans le cadre d'un système européen de certification de cybersécurité qui accorde un degré substantiel de fiabilité aux qualités de cybersécurité revendiquées ou prétendues d'un ***processus,*** produit ou service TIC, et caractérisé sur la base de spécifications techniques, normes et procédures y

afférents, y compris les contrôles techniques, dont l'objectif est de réduire substantiellement le risque d'incidents de cybersécurité;

afférents, y compris les contrôles techniques, dont l'objectif est de réduire substantiellement le risque d'incidents de cybersécurité;

Amendement 78

Proposition de règlement
Article 46 – paragraphe 2 – point c

Texte proposé par la Commission	*Amendement*
(c) le niveau d'assurance ***élevé*** renvoie à un certificat délivré dans le cadre d'un système européen de certification de cybersécurité qui accorde un degré de fiabilité aux qualités de cybersécurité revendiquées ou prétendues d'un produit ou service TIC plus élevé que les certificats ayant le niveau d'assurance ***substantiel***, et caractérisé sur la base de spécifications techniques, normes et procédures y afférents, y compris les contrôles techniques, dont l'objectif est de prévenir les incidents de cybersécurité;	(c) le niveau d'assurance ***«élevé»*** renvoie à un certificat délivré dans le cadre d'un système européen de certification de cybersécurité qui accorde un degré de fiabilité aux qualités de cybersécurité revendiquées ou prétendues d'un ***processus,*** produit ou service TIC plus élevé que les certificats ayant le niveau d'assurance ***«substantiel»***, et caractérisé sur la base de spécifications techniques, normes et procédures y afférents, y compris les contrôles techniques, dont l'objectif est de prévenir les incidents de cybersécurité; ***cela s'applique en particulier aux produits et services destinés à être utilisés par les opérateurs de services essentiels, au sens de l'article 4, paragraphe 4, de la directive (UE) 2016/1148.***

Amendement 79

Proposition de règlement
Article 47 – paragraphe 1 – partie introductive

Texte proposé par la Commission	*Amendement*
1. ***Un*** système européen de certification de cybersécurité comprend les éléments suivants:	1. ***Chaque*** système européen de certification de cybersécurité comprend ***au moins*** les éléments suivants***, le cas échéant***:

Amendement 80

Proposition de règlement
Article 47 – paragraphe 1 – point a

Texte proposé par la Commission	*Amendement*
(a) l'objet et le champ d'application ***de la*** certification, notamment le type ou les catégories de produits et services TIC;	(a) l'objet et le champ d'application ***du système de*** certification, notamment ***tout secteur spécifique couvert et*** le type ou les catégories de produits et services TIC;

Amendement 81

Proposition de règlement
Article 47 – paragraphe 1 – point b

Texte proposé par la Commission	*Amendement*
(b) une description détaillée des exigences de cybersécurité utilisées pour évaluer les produits et services TIC, ***par exemple*** par référence aux normes ou spécifications techniques européennes ou ***internationales***;	(b) une description détaillée des exigences de cybersécurité utilisées pour évaluer les produits et services TIC, ***notamment*** par référence aux normes ou spécifications techniques ***internationales,*** européennes ou ***nationales***;

Amendement 82

Proposition de règlement
Article 47 – paragraphe 1 – point b bis (nouveau)

Texte proposé par la Commission	*Amendement*
	(b bis) mention détaillée lorsqu'une certification accordée ne peut s'appliquer qu'à un produit particulier ou peut s'appliquer à une gamme de produits, par exemple, différentes versions ou différents modèles de la même structure de produit de base;

Amendement 83

Proposition de règlement
Article 47 – paragraphe 1 – point c bis (nouveau)

Texte proposé par la Commission	*Amendement*
	(c bis) indication précisant si l'autodéclaration de conformité est autorisée dans le cadre du système, et la procédure applicable à l'évaluation de la conformité ou à l'autodéclaration de conformité ou aux deux;

Amendement 84

Proposition de règlement
Article 47 – paragraphe 1 – point c ter (nouveau)

Texte proposé par la Commission	*Amendement*
	(c ter) exigences de certification, définies de telle manière que la certification puisse être intégrée dans, ou reposer sur, les processus de cybersécurité systématiques du producteur, suivis pendant la conception, l'élaboration et le cycle de vie du processus, produit ou service TIC;

Amendement 85

Proposition de règlement
Article 47 – paragraphe 1 – point f

Texte proposé par la Commission	*Amendement*
(f) lorsque le système prévoit des marques ou des labels, les conditions dans lesquelles ces marques ou labels peuvent être utilisés;	(f) lorsque le système prévoit des marques ou des labels, ***par exemple, un label UE de conformité de la cybersécurité signifiant que le processus, produit ou service TIC satisfait aux critères d'un système,*** les conditions dans lesquelles ces marques ou labels peuvent être utilisés;

Amendement 86

Proposition de règlement
Article 47 – paragraphe 1 – point g

Texte proposé par la Commission	*Amendement*
(g) ***lorsque le système comprend une surveillance, les*** modalités relatives au contrôle du respect des exigences associées aux certificats, notamment les mécanismes permettant de démontrer le respect constant des exigences de cybersécurité***;***	(g) ***les*** modalités relatives au contrôle du respect des exigences associées aux certificats, notamment les mécanismes permettant de démontrer le respect constant des exigences de cybersécurité ***précises, telles que des mises à jour, mises à niveau ou correctifs obligatoires du processus, produit ou service TIC concerné, sous réserve de pertinence et de faisabilité.***

Amendement 87

Proposition de règlement
Article 47 – paragraphe 1 – point h

Texte proposé par la Commission	*Amendement*
(h) les conditions permettant de délivrer, maintenir et poursuivre la certification et d'étendre ou de réduire son champ d'application;	(h) les conditions permettant de délivrer, maintenir et poursuivre***, renouveler*** la certification et d'étendre ou de réduire son champ d'application;

Amendement 88

Proposition de règlement
Article 47 – paragraphe 1 – point i

Texte proposé par la Commission	*Amendement*
(i) les règles relatives aux conséquences de la non-conformité ***des*** produits ***et*** services TIC certifiés aux exigences en matière de certification;	(i) les règles relatives aux conséquences de la non-conformité ***de*** produits ***et*** services TIC certifiés aux exigences en matière de certification***, et des informations générales sur les sanctions prévues à l'article 54 du présent règlement***;

Amendement 89

Proposition de règlement
Article 47 – paragraphe 1 – point j

Texte proposé par la Commission	*Amendement*
(j) les règles relatives aux modalités de signalement et de traitement des vulnérabilités de cybersécurité non détectées précédemment dans des produits et services TIC;	(j) les règles relatives aux modalités de signalement et de traitement des vulnérabilités de cybersécurité non détectées précédemment dans des produits et services TIC***, notamment au moyen de processus de divulgation coordonnée des vulnérabilités***;

Amendement 90

Proposition de règlement
Article 47 – paragraphe 1 – point l

Texte proposé par la Commission	*Amendement*
(l) ***l'identification*** des systèmes nationaux de certification de cybersécurité couvrant le même type ou les mêmes catégories de produits et services TIC;	(l) ***l'identification*** des systèmes nationaux ***ou internationaux*** de certification de cybersécurité***, ou des accords internationaux de reconnaissance mutuelle existants,*** couvrant le même type ou les mêmes catégories de produits et services TIC;

Amendement 91

Proposition de règlement
Article 47 – paragraphe 1 – point m bis (nouveau)

Texte proposé par la Commission	*Amendement*
	m bis) durée maximale de validité des certificats;

Amendement 92

Proposition de règlement
Article 47 – paragraphe 1 – point m ter (nouveau)

Texte proposé par la Commission	*Amendement*
	(m ter) règles sur les tests de résistance et de résilience pour le niveau d'assurance «élevé»;

Amendement 93

Proposition de règlement
Article 47 – paragraphe 3

Texte proposé par la Commission	*Amendement*
3. Lorsqu'un acte spécifique de l'Union le prévoit, la certification au titre d'un système européen de certification de cybersécurité peut être utilisée pour démontrer la présomption de conformité aux exigences de cet acte.	3. Lorsqu'un ***futur*** acte spécifique de l'Union le prévoit, la certification au titre d'un système européen de certification de cybersécurité peut être utilisée pour démontrer la présomption de conformité aux exigences de cet acte.

Amendement 94

Proposition de règlement
Article 48 – paragraphe 2

Texte proposé par la Commission	*Amendement*
2. La certification est volontaire, sauf indication contraire dans le droit de l'Union.	2. ***La certification au titre d'un système européen de certification de cybersécurité est obligatoire pour les produits et services TIC comportant un risque inhérent élevé spécifiquement qui sont destinés à être utilisés par les opérateurs de services essentiels définis à l'article 4, paragraphe 4, de la directive (UE) 2016/1148. En ce qui concerne tous les autres produits et services TIC, la certification*** est volontaire, sauf indication contraire dans le droit de l'Union.

Amendement 95

Proposition de règlement
Article 48 – paragraphe 3

Texte proposé par la Commission	*Amendement*
3. Les organismes d'évaluation de la conformité visés à l'article 51 délivrent ***un certificat européen*** de cybersécurité au titre du présent article sur la base des critères figurant dans le système européen de certification de cybersécurité adopté conformément à l'article 44.	3. Les organismes d'évaluation de la conformité visés à l'article 51 délivrent ***des certificats européens*** de cybersécurité au titre du présent article sur la base des critères figurant dans le système européen de certification de cybersécurité adopté conformément à l'article 44. ***En lieu et place de la certification des organes d'évaluation de la conformité, les fabricants de produits et les fournisseurs de services peuvent, lorsque le système en question prévoit cette possibilité, effectuer une autodéclaration mentionnant qu'un processus, produit ou service satisfait aux critères du système de certification. Dans ce cas, le fabricant du produit ou le fournisseur du service transmet, sur demande, l'autodéclaration de conformité à l'autorité nationale de contrôle de la certification requérante et à l'ENISA.***

Amendement 96

Proposition de règlement
Article 48 – paragraphe 4 – partie introductive

Texte proposé par la Commission	*Amendement*
4. Par dérogation au paragraphe 3, dans des cas dûment justifiés, un système européen de cybersécurité particulier peut prévoir que seul un organisme public puisse délivrer un certificat européen de cybersécurité dans le cadre dudit système. Cet organisme public est l'une des entités suivantes:	4. Par dérogation au paragraphe 3, dans des cas dûment justifiés, ***tels que des raisons de sécurité nationale,*** un système européen ***de certification*** de cybersécurité particulier peut prévoir que seul un organisme public puisse délivrer un certificat européen de cybersécurité dans le cadre dudit système. Cet organisme public est l'une des entités suivantes:

Amendement 97

Proposition de règlement
Article 48 – paragraphe 5

Texte proposé par la Commission	*Amendement*
5. ***2012. La*** personne physique ou morale qui soumet ses produits ou services TIC au mécanisme de certification fournit à l'organisme d'évaluation de la conformité visé à l'article 51 toutes les informations nécessaires pour mener la procédure de certification.	5. ***La*** personne physique ou morale qui soumet ses produits ou services TIC au mécanisme de certification fournit à l'organisme d'évaluation de la conformité visé à l'article 51 toutes les informations nécessaires pour mener la procédure de certification***, notamment les informations sur toute vulnérabilité connue en matière de sécurité***.

Amendement 98

Proposition de règlement
Article 48 – paragraphe 6

Texte proposé par la Commission	*Amendement*
6. Les certificats sont délivrés pour une durée maximale ***de trois ans*** et peuvent être renouvelés dans les mêmes conditions pourvu que les exigences applicables continuent d'être satisfaites.	6. Les certificats sont délivrés ***et restent valables*** pour une durée maximale ***fixée dans chaque système de certification*** et peuvent être renouvelés dans les mêmes conditions***,*** pourvu que les exigences applicables ***dans ce système, y compris les exigences révisées ou modifiées,*** continuent d'être satisfaites.

Amendement 99

Proposition de règlement
Article 48 – paragraphe 6 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	6 bis. Les certificats restent valables pour toutes les nouvelles versions d'un processus, produit ou service, lorsque la nouvelle version entend principalement corriger, réparer ou pallier par tout autre moyen des vulnérabilités ou des menaces de sécurité connues ou potentielles.

Amendement 100

Proposition de règlement
Article 49 – paragraphe 1

Texte proposé par la Commission	*Amendement*
1. Sans préjudice du paragraphe 3, les systèmes nationaux de certification de cybersécurité et les procédures connexes pour les produits et services TIC couverts par un système européen de certification de cybersécurité cessent de produire leurs effets à partir de la date fixée dans l'acte ***d'exécution*** adopté en application de l'article 44, paragraphe 4. Les systèmes nationaux de certification de cybersécurité existants et les procédures connexes pour les produits et services TIC qui ne sont pas couverts par un système européen de certification de cybersécurité continuent à exister.	***1.*** Sans préjudice du paragraphe 3, les systèmes nationaux de certification de cybersécurité et les procédures connexes pour les produits et services TIC couverts par un système 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 44, paragraphe 4. ***La Commission contrôle le respect du présent alinéa dans le souci d'éviter l'existence de systèmes parallèles.*** Les systèmes nationaux de certification de cybersécurité existants et les procédures connexes pour les produits et services TIC qui ne sont pas couverts par un système européen de certification de cybersécurité continuent à exister.

Amendement 101

Proposition de règlement
Article 49 – paragraphe 3

Texte proposé par la Commission	*Amendement*
3. Les certificats existants, délivrés en vertu de systèmes nationaux de certification de cybersécurité***,*** restent valables jusqu'à leur date d'expiration.	3. Les certificats existants, délivrés en vertu de systèmes nationaux de certification de cybersécurité ***qui sont couverts par un système européen de certification de cybersécurité*** restent valables jusqu'à leur date d'expiration.

Amendement 102

Proposition de règlement
Article 50 – paragraphe 3

Texte proposé par la Commission	*Amendement*
3. Chaque autorité nationale de	3. Chaque autorité nationale de

contrôle de la certification est indépendante, en ce qui concerne son organisation, ses décisions de financement, sa structure juridique et son processus décisionnel, des entités qu'elle surveille.	contrôle de la certification est indépendante, en ce qui concerne son organisation, ses décisions de financement, sa structure juridique et son processus décisionnel, des entités qu'elle surveille***, et ne peut être ni un organisme d'évaluation de la conformité ni un organisme national d'accréditation***.

Amendement 103

Proposition de règlement
Article 50 – paragraphe 6 – point a

Texte proposé par la Commission	*Amendement*
(a) contrôlent et assurent l'application des dispositions du présent titre au niveau national et supervisent la conformité ***des certificats qui ont été délivrés*** par ***les organismes d'évaluation*** de ***la conformité établis sur leur territoire aux exigences énoncées dans le présent titre et dans le système européen de certification de cybersécurité correspondant;***	(a) contrôlent et assurent l'application des dispositions du présent titre au niveau national et supervisent la conformité***, dans le respect des règles adoptées*** par ***le groupe européen*** de ***certification de cybersécurité conformément à l'article 53, paragraphe 3, point d bis), en ce qui concerne:*** ***i) les certificats délivrés par les organismes d'évaluation de la conformité établis sur leur territoire aux exigences énoncées dans le présent titre et dans le système européen de certification de cybersécurité correspondant; et*** ***ii) les autodéclarations de conformité effectuées dans le cadre du système d'un processus, produit ou service TIC;***

Amendement 104

Proposition de règlement
Article 50 – paragraphe 6 – point b

Texte proposé par la Commission	*Amendement*
(b) contrôlent et ***supervisent*** les activités des organismes d'évaluation de la conformité aux fins du présent règlement, notamment en ce qui concerne la notification des organismes d'évaluation de	(b) contrôlent***, supervisent*** et***, au moins tous les deux ans, évaluent*** les activités des organismes d'évaluation de la conformité aux fins du présent règlement, notamment en ce qui concerne la

la conformité et des missions connexes énoncées à l'article 52 du présent règlement;	notification des organismes d'évaluation de la conformité et des missions connexes énoncées à l'article 52 du présent règlement;

Amendement 105

Proposition de règlement
Article 50 – paragraphe 6 – point c

Texte proposé par la Commission	*Amendement*
(c) traitent les réclamations introduites par une personne physique ou morale en rapport avec les certificats délivrés par des organismes d'évaluation de la conformité établis sur leur territoire, examinent l'objet de la réclamation dans la mesure nécessaire et informent l'auteur de la réclamation de l'état d'avancement et de l'issue de l'enquête dans un délai raisonnable;	(c) traitent les réclamations introduites par une personne physique ou morale en rapport avec les certificats délivrés par des organismes d'évaluation de la conformité établis sur leur territoire ***ou les autodéclarations de conformité effectuées***, examinent l'objet de la réclamation dans la mesure nécessaire et informent l'auteur de la réclamation de l'état d'avancement et de l'issue de l'enquête dans un délai raisonnable;

Amendement 106

Proposition de règlement
Article 50 – paragraphe 6 – point c bis (nouveau)

Texte proposé par la Commission	*Amendement*
	(c bis) transmettent à l'ENISA et au groupe européen de certification de cybersécurité les résultats des vérifications visées au point a) et les évaluations visées au point b);

Amendement 107

Proposition de règlement
Article 50 – paragraphe 6 – point d

Texte proposé par la Commission	*Amendement*
(d) coopèrent avec les autres autorités	(d) coopèrent avec les autres autorités

nationales de contrôle de la certification ou d'autres autorités publiques, notamment en partageant des informations sur l'éventuelle non-conformité de produits et services TIC aux exigences du présent règlement ou à celles de systèmes de certification de cybersécurité spécifiques;	nationales de contrôle de la certification***, les organismes nationaux d'accréditation*** ou d'autres autorités publiques, notamment en partageant des informations sur l'éventuelle non-conformité***, y compris les déclarations de certification trompeuses, fausses ou frauduleuses,*** de produits et services TIC aux exigences du présent règlement ou à celles de systèmes de certification de cybersécurité spécifiques;

Amendement 108

Proposition de règlement
Article 50 – paragraphe 7 – point c bis (nouveau)

Texte proposé par la Commission	*Amendement*
	(c bis) retirer l'accréditation des organismes nationaux de conformité qui ne respectent pas le présent règlement.

Amendement 109

Proposition de règlement
Article 50 – paragraphe 7 – point e

Texte proposé par la Commission	*Amendement*
(e) retirer, conformément au droit national, les certificats qui ne sont pas conformes au présent règlement ou à un système européen de certification de cybersécurité;	(e) retirer, conformément au droit national, les certificats qui ne sont pas conformes au présent règlement ou à un système européen de certification de cybersécurité ***et informer les organismes nationaux d'accréditation en conséquence***;

Amendement 110

Proposition de règlement
Article 50 – paragraphe 7 – point f bis (nouveau)

Texte proposé par la Commission	*Amendement*
	(f bis) proposer à l'ENISA des experts

pour participer au groupe d'experts pour la consultation des parties prenantes visé à l'article 44, paragraphe 2.

Amendement 111

Proposition de règlement
Article 50 – paragraphe 8 - alinéa 1 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	La Commission met à disposition un système de soutien général à l'information électronique aux fins de cet échange.

Amendement 112

Proposition de règlement
Article 50 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	Article 50 bis
	Examen par les pairs
	1. Les autorités nationales de contrôle de la certification font l'objet d'un examen par les pairs en ce qui concerne les activités qu'elles exercent au titre de l'article 50 du présent règlement.
	2. L'examen par les pairs couvre les évaluations des procédures mises en place par les autorités nationales de contrôle de la certification, notamment les procédures de contrôle de la conformité des produits soumis à la certification de cybersécurité, la compétence du personnel, la régularité des contrôles et la méthode d'inspection, ainsi que l'exactitude des résultats. L'examen par les pairs détermine également si les autorités nationales de contrôle de la certification en question disposent de ressources suffisantes pour la bonne exécution de leurs tâches, comme l'exige l'article 50, paragraphe 4.

3. L'examen par les pairs d'une autorité nationale de contrôle de la certification est effectué par deux autorités nationales de contrôle de la certification d'autres États membres et la Commission, au minimum une fois tous les cinq ans. L'ENISA peut participer à l'examen par les pairs et décide de sa participation sur la base d'une analyse des risques.

4. La Commission est habilitée à adopter des actes délégués, conformément à l'article 55 bis, afin d'établir un plan pour l'examen par les pairs couvrant une période d'au moins cinq ans, définissant des critères concernant la composition de l'équipe chargée de l'examen par les pairs, la méthode utilisée pour mener cet examen, le programme, la périodicité et les autres tâches y relatives. Lors de l'adoption de ces actes délégués, la Commission tient dûment compte des observations formulées par le groupe.

5. Le groupe examine les conclusions de l'examen par les pairs. L'ENISA produit un résumé des conclusions qu'elle rend public.

Amendement 113

Proposition de règlement
Article 51 – paragraphe 2 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	2 bis. Lorsque les fabricants optent pour l'«autodéclaration de conformité», conformément à l'article 48, paragraphe 3, les organismes d'évaluation de la conformité prennent des mesures supplémentaires, afin de vérifier les procédures internes qu'a engagées le fabricant à l'effet de s'assurer que ses produits ou services satisfont aux exigences du système européen de certification de cybersécurité.

Amendement 114

Proposition de règlement
Article 53 – paragraphe 3 – point d bis (nouveau)

Texte proposé par la Commission	*Amendement*
	(d bis) d'adopter des règles contraignantes précisant les intervalles auxquels les autorités nationales de contrôle de la certification doivent procéder à des vérifications des certificats et les critères, l'ampleur et la portée de ces vérifications, et d'arrêter des règles et normes communes en ce qui concerne la transmission des résultats prévue à l'article 50, paragraphe 6;

Amendement 115

Proposition de règlement
Article 53 – paragraphe 3 – point e

Texte proposé par la Commission	*Amendement*
(e) d'examiner les évolutions pertinentes dans le domaine de la certification de cybersécurité et de l'échange de bonnes pratiques sur les systèmes de certification de cybersécurité;	(e) d'examiner les évolutions pertinentes dans le domaine de la certification de cybersécurité et de l'échange ***d'informations et*** de bonnes pratiques sur les systèmes de certification de cybersécurité;

Amendement 116

Proposition de règlement
Article 53 – paragraphe 3 – point f bis (nouveau)

Texte proposé par la Commission	*Amendement*
	(f bis) d'échanger les bonnes pratiques en ce qui concerne les enquêtes des organismes d'évaluation de la conformité, les titulaires de certificats européens de cybersécurité et les fournisseurs de services ayant effectué des

autodéclarations de conformité;

Amendement 117

Proposition de règlement
Article 53 – paragraphe 3 – point f ter (nouveau)

Texte proposé par la Commission	*Amendement*
	(f ter) de faciliter l'alignement des systèmes européens de certification de cybersécurité sur les normes internationalement reconnues et, le cas échéant, de recommander à l'ENISA des domaines dans lesquels elle devrait nouer le dialogue avec les organisations de normalisation internationales et européennes concernées, afin de remédier aux insuffisances et aux lacunes en matière de normes internationalement reconnues;

Amendement 118

Proposition de règlement
Article 53 – paragraphe 3 – point f quater (nouveau)

Texte proposé par la Commission	*Amendement*
	(f quater) de conseiller l'ENISA, lors de l'établissement du programme de travail visé à l'article 43 bis, sur une liste prioritaire des produits et services TIC pour lesquels, selon elle, une certification de cybersécurité européenne est requise;

Amendement 119

Proposition de règlement
Article 53 – paragraphe 4 – alinéa 1 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	L'ENISA veille à ce que l'ordre du jour, le procès-verbal et le relevé des décisions adoptées soient dressés et à ce que les

versions publiées de ces documents soient mises à la disposition du public sur son site internet après chaque réunion du groupe.

Amendement 120

Proposition de règlement
Article 55 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	Article 55 bis
	Exercice de la délégation
	Le pouvoir d'adopter des actes délégués conféré à la Commission est soumis aux conditions fixées au présent article.
	Le pouvoir d'adopter des actes délégués visé à l'article 44, paragraphe 4, et à l'article 50 bis, paragraphe 4, est conféré à la Commission pour une période de cinq ans à compter de [la date d'entrée en vigueur de l'acte législatif de base]. 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.
	La délégation de pouvoir visée à l'article 44, paragraphe 4, et à l'article 50 bis, paragraphe 4, 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 la 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.

Avant d'adopter 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».

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

Un acte délégué adopté en vertu de l'article 44, paragraphe 4, ou de l'article 50 bis, paragraphe 4, 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.

PROCÉDURE DE LA COMMISSION SAISIE POUR AVIS

Titre	Règlement relatif à l'ENISA, Agence de l'Union européenne pour la cybersécurité, et abrogeant le règlement (UE) no 526/2013, et relatif à la certification des technologies de l'information et des communications en matière de cybersécurité (règlement sur la cybersécurité)
Références	COM(2017)0477 – C8-0310/2017 – 2017/0225(COD)
Commission compétente au fond Date de l'annonce en séance	ITRE 23.10.2017
Avis émis par Date de l'annonce en séance	IMCO 23.10.2017
Commissions associées - date de l'annonce en séance	18.1.2018
Rapporteur(e) pour avis Date de la nomination	Nicola Danti 25.9.2017
Examen en commission	21.2.2018 21.3.2018
Date de l'adoption	17.5.2018
Résultat du vote final	+: 31 –: 2 0: 1
Membres présents au moment du vote final	John Stuart Agnew, Pascal Arimont, Dita Charanzová, Carlos Coelho, Anna Maria Corazza Bildt, Daniel Dalton, Nicola Danti, Dennis de Jong, Pascal Durand, Evelyne Gebhardt, Robert Jarosław Iwaszkiewicz, Liisa Jaakonsaari, Marlene Mizzi, Nosheena Mobarik, Jiří Pospíšil, Andreas Schwab, Olga Sehnalová, Jasenko Selimovic, Ivan Štefanec, Catherine Stihler, Mylène Troszczynski, Mihai Ţurcanu, Anneleen Van Bossuyt, Marco Zullo
Suppléants présents au moment du vote final	Jan Philipp Albrecht, Kaja Kallas, Arndt Kohn, Emma McClarkin, Adam Szejnfeld, Marc Tarabella, Lambert van Nistelrooij, Kerstin Westphal
Suppléants (art. 200, par. 2) présents au moment du vote final	Inés Ayala Sender, Flavio Zanonato

VOTE FINAL PAR APPEL NOMINAL EN COMMISSION SAISIE POUR AVIS

31	+
ALDE	Dita Charanzová, Kaja Kallas, Jasenko Selimovic
ECR	Daniel Dalton, Emma McClarkin, Nosheena Mobarik, Anneleen Van Bossuyt
EFDD	Marco Zullo
GUE/NGL	Dennis de Jong
PPE	Pascal Arimont, Carlos Coelho, Anna Maria Corazza Bildt, Jiří Pospíšil, Andreas Schwab, Ivan Štefanec, Adam Szejnfeld, Mihai Ţurcanu, Lambert van Nistelrooij
S&D	Inés Ayala Sender, Nicola Danti, Evelyne Gebhardt, Liisa Jaakonsaari, Arndt Kohn, Marlene Mizzi, Olga Sehnalová, Catherine Stihler, Marc Tarabella, Kerstin Westphal, Flavio Zanonato
Verts/ALE	Jan Philipp Albrecht, Pascal Durand

2	-
EFDD	John Stuart Agnew, Robert Jarosław Iwaszkiewicz

1	0
ENF	Mylène Troszczynski

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