Parlement européen
2019-2024

Commission du marché intérieur et de la protection des consommateurs

2022/0272(COD)

30.6.2023

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 concernant des exigences horizontales en matière de cybersécurité pour les produits comportant des éléments numériques et modifiant le règlement (UE) 2019/1020
(COM(2022)0454 – C9-0308/2022 – 2022/0272(COD))

Rapporteur pour avis (*): Morten Løkkegaard

(*) Commission associée – article 57 du règlement intérieur

PA_Legam

JUSTIFICATION SUCCINCTE

Le rapporteur, en tant qu'ancien rapporteur pour avis de la commission IMCO sur la directive SRI 2, considère que la législation sur la cyberrésilience est une prochaine étape essentielle et incontournable pour améliorer la cybersécurité de l'Union européenne. Conscient que, par définition, la cybersécurité ne sera jamais totale à 100 %, le rapporteur est d'avis qu'il importe de faire tout ce qui est en notre pouvoir pour réduire le nombre de vulnérabilités dans l'Union; à cet égard, la législation sur la cyberrésilience est une prochaine étape qui vient à point nommé. Nous devons renforcer la cybersécurité des produits comportant des éléments numériques et d'autres nouveaux produits tels que les appareils de l'internet des objets qui font désormais partie intégrante de la vie quotidienne des consommateurs et des entreprises en Europe.

La commission IMCO étant compétente pour le fonctionnement et la mise en œuvre du marché unique ainsi que pour les règles relatives à la protection des consommateurs, le rapporteur a cherché à introduire des amendements qui visent à améliorer le fonctionnement du marché intérieur tout en prévoyant un niveau élevé de protection des consommateurs dans le cadre de la proposition, en particulier en ce qui concerne les exigences en matière de cybersécurité pour les produits comportant des éléments numériques.

Le rapporteur estime, en outre, que certains aspects du règlement proposé doivent être améliorés afin de garantir une clarté juridique et une cohérence entre les dispositions pertinentes dudit règlement et d'autres actes législatifs. Il s'agit en particulier de la directive SRI 2, du règlement récemment adopté sur la sécurité générale des produits, du règlement sur l'intelligence artificielle et du règlement relatif aux machines et équipements, ainsi que d'un certain nombre d'actes délégués et d'actes d'exécution. Ainsi, le rapporteur propose des amendements qui visent à améliorer la clarté juridique et à contribuer à garantir une interprétation et une application cohérentes, effectives et uniformes des actes législatifs susmentionnés.

De plus, les micro, petites et moyennes entreprises étant des acteurs économiques essentiels sur le marché numérique, le rapporteur introduit un certain nombre d'amendements visant à simplifier les formalités administratives et à limiter la charge administrative pesant sur les petites entreprises, sans abaisser le niveau de sécurité. En outre, le rapporteur introduit des amendements visant à garantir que les microentreprises et les PME bénéficient d'orientations et de conseils spécifiques pour satisfaire aux exigences de la législation sur la cyberrésilience.

Enfin, le rapporteur introduit des amendements dont l'objectif est d'assurer une communication plus efficace avec les autorités compétentes (autorités nationales de surveillance du marché, ENISA), ainsi que de renforcer les dispositions relatives aux obligations et aux compétences des autorités concernées en ce qui concerne les plaintes, les inspections et les activités conjointes. Par ailleurs, certains amendements présentés par le rapporteur portent en particulier sur l'amélioration des exigences en matière de cybersécurité pour les composants intégrés dans des produits finis comportant des éléments numériques, en précisant les obligations des opérateurs économiques tels que les fabricants et les mandataires.

Le rapporteur réaffirme que l'introduction de la législation sur la cyberrésilience est une étape qui vient à point nommé et qui est incontournable pour renforcer la lutte contre les menaces en matière de cybersécurité dans l'Union. Dans ses propositions d'amendements, le

rapporteur s'efforce de trouver un juste équilibre entre la garantie d'un niveau accru de cybersécurité dans l'intérêt des consommateurs européens et une charge proportionnée pour les milieux économiques. Le rapporteur vise à ce que la cybersécurité devienne un paramètre naturel de la concurrence sur le marché intérieur. C'est dans cet esprit qu'il a cherché à adapter la proposition.

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 ce qui suit:

Amendement 1

Proposition de règlement
Considérant 1

Texte proposé par la Commission	*Amendement*
(1) Il est nécessaire d'améliorer le fonctionnement du marché intérieur en ***établissant*** un cadre juridique uniforme concernant les exigences essentielles en matière de cybersécurité aux fins de la mise sur le marché de l'Union de produits comportant des éléments numériques. Deux problèmes majeurs représentant des coûts supplémentaires pour les utilisateurs et la société devraient être réglés: d'une part, le niveau de cybersécurité des produits comportant des éléments numériques est faible, comme en témoignent les vulnérabilités généralisées et le manque de mises à jour de sécurité déployées de manière cohérente pour y remédier, et, d'autre part, les utilisateurs n'ont pas suffisamment accès aux informations et ne les comprennent pas bien, ce qui les empêche de choisir des produits dotés de propriétés de cybersécurité adéquates ou de les utiliser de manière sécurisée.	(1) Il est nécessaire d'améliorer le fonctionnement du marché intérieur ***tout*** en ***garantissant*** un ***niveau élevé de protection des consommateurs et de cybersécurité grâce à l'établissement d'un*** cadre juridique uniforme concernant les exigences essentielles en matière de cybersécurité aux fins de la mise sur le marché de l'Union de produits comportant des éléments numériques. Deux problèmes majeurs représentant des coûts supplémentaires pour les utilisateurs et la société devraient être réglés: d'une part, le niveau de cybersécurité des produits comportant des éléments numériques est faible, comme en témoignent les vulnérabilités généralisées et le manque de mises à jour de sécurité déployées de manière cohérente pour y remédier, et, d'autre part, les utilisateurs n'ont pas suffisamment accès aux informations et ne les comprennent pas bien, ce qui les empêche de choisir des produits dotés de propriétés de cybersécurité adéquates ou de les utiliser de manière sécurisée.

Amendement 2

Proposition de règlement
Considérant 7

Texte proposé par la Commission	*Amendement*
(7) Dans certaines conditions, tous les produits comportant des éléments numériques intégrés ou connectés à un système d'information électronique plus vaste peuvent servir de vecteur d'attaque pour des acteurs malveillants. En conséquence, même le matériel et les logiciels considérés comme moins critiques peuvent faciliter une première compromission d'un appareil ou d'un réseau, permettant à des acteurs malveillants d'obtenir un accès privilégié à un système ou de se déplacer latéralement entre différents systèmes. Les fabricants devraient donc veiller à ce que tous les produits ***connectables*** comportant des éléments numériques soient conçus et développés conformément aux exigences essentielles énoncées dans le présent règlement. Cela comprend à la fois les produits qui peuvent être connectés physiquement via des interfaces matérielles et les produits qui sont connectés logiquement, notamment par des connecteurs logiciels, tuyauteries, fichiers, interfaces de programmation d'application ou tout autre type d'interface logicielle. Étant donné que les menaces de cybersécurité peuvent se propager via divers produits comportant des éléments numériques avant d'atteindre une cible donnée, par exemple en enchaînant plusieurs exploits de vulnérabilité, les fabricants devraient également assurer la cybersécurité des produits qui ne sont connectés qu'indirectement à d'autres dispositifs ou réseaux.	(7) Dans certaines conditions, tous les produits comportant des éléments numériques intégrés ou connectés à un système d'information électronique plus vaste peuvent servir de vecteur d'attaque pour des acteurs malveillants. En conséquence, même le matériel et les logiciels considérés comme moins critiques peuvent faciliter une première compromission d'un appareil ou d'un réseau, permettant à des acteurs malveillants d'obtenir un accès privilégié à un système ou de se déplacer latéralement entre différents systèmes. Les fabricants devraient donc veiller à ce que tous les produits comportant des éléments numériques ***connectés à un réseau ou dispositif externe*** soient conçus et développés conformément aux exigences essentielles énoncées dans le présent règlement. Cela comprend à la fois les produits qui peuvent être connectés physiquement ***à des réseaux ou dispositifs externes*** via des interfaces matérielles et les produits qui sont connectés logiquement, notamment par des connecteurs logiciels, tuyauteries, fichiers, interfaces de programmation d'application ou tout autre type d'interface logicielle. Étant donné que les menaces de cybersécurité peuvent se propager via divers produits comportant des éléments numériques avant d'atteindre une cible donnée, par exemple en enchaînant plusieurs exploits de vulnérabilité, les fabricants devraient également assurer la cybersécurité des produits qui ne sont connectés qu'indirectement à d'autres dispositifs ou réseaux.

Amendement 3

Proposition de règlement
Considérant 7 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	(7 bis) Le présent règlement n'a pas vocation à s'appliquer aux réseaux internes d'un produit comportant des éléments numériques si ces réseaux possèdent des points terminaux dédiés et sont complètement isolés et sécurisés par rapport à une connexion externe.

Amendement 4

Proposition de règlement
Considérant 7 ter (nouveau)

Texte proposé par la Commission	*Amendement*
	(7 ter) Le présent règlement ne devrait pas s'appliquer aux pièces de rechange destinées exclusivement à remplacer les pièces défectueuses de produits comportant des éléments numériques en vue de restaurer leur fonctionnalité.

Amendement 5

Proposition de règlement
Considérant 9

Texte proposé par la Commission	*Amendement*
(9) Le présent règlement garantit un niveau élevé de cybersécurité des produits comportant des éléments numériques. Il ne réglemente pas les services, tels que le logiciel en tant que service (SaaS)***, à l'exception des solutions de traitement de données à distance relatives à un produit comportant des éléments numériques, par lesquelles on entend tout traitement de données à distance pour lequel le logiciel est conçu et développé par le fabricant du produit concerné ou sous la responsabilité***	(9) Le présent règlement garantit un niveau élevé de cybersécurité des produits comportant des éléments numériques. Il ne réglemente pas les services, tels que le logiciel en tant que service (SaaS). La [directive XXX/XXXX (SRI 2)] met en place des exigences en matière de cybersécurité et de signalement des incidents pour les entités essentielles et importantes, telles que les infrastructures critiques, en vue d'accroître la résilience des services qu'elles fournissent. La

de celui-ci, et dont l'absence empêcherait ledit produit d'exécuter l'une de ses fonctions. La [directive XXX/XXXX (SRI 2)] met en place des exigences en matière de cybersécurité et de signalement des incidents pour les entités essentielles et importantes, telles que les infrastructures critiques, en vue d'accroître la résilience des services qu'elles fournissent. La [directive XXX/XXXX (SRI 2)] s'applique aux services d'informatique en nuage et aux modèles de services en nuage, tels que le SaaS. Toutes les entités fournissant des services d'informatique en nuage dans l'Union**,** qui atteignent ou dépassent le seuil fixé pour les entreprises de taille moyenne relèvent du champ d'application de cette directive.

[directive XXX/XXXX (SRI 2)] s'applique aux services d'informatique en nuage et aux modèles de services en nuage, tels que le SaaS. Toutes les entités fournissant des services d'informatique en nuage dans l'Union qui atteignent ou dépassent le seuil fixé pour les entreprises de taille moyenne relèvent du champ d'application de cette directive.

Amendement 6

Proposition de règlement
Considérant 10

Texte proposé par la Commission	*Amendement*
(10) Afin de ne pas entraver l'innovation ou la recherche, les logiciels libres et ouverts développés ou fournis en dehors du cadre d'une activité commerciale ne devraient pas être couverts par le présent règlement. C'est notamment le cas des logiciels, y compris leurs codes sources et versions modifiées, qui sont librement partagés et accessibles, utilisables, modifiables et redistribuables. ***En ce qui concerne le logiciel, l'activité commerciale*** peut être caractérisée ***non seulement*** par le prix facturé pour un ***produit***, mais également par le prix des services d'assistance technique, par la fourniture d'une plate-forme logicielle par l'intermédiaire de laquelle le fabricant monétise d'autres services, ou par l'utilisation de données à caractère personnel pour des raisons autres qu'aux seules fins d'améliorer la sécurité, la compatibilité ou l'interopérabilité du	(10) ***Les logiciels et les données qui sont librement partagés, auxquels les utilisateurs peuvent librement accéder et qu'ils peuvent librement utiliser, modifier et redistribuer, y compris leurs versions modifiées, peuvent contribuer à la recherche et à l'innovation sur le marché. Des recherches menées par la Commission montrent également que les logiciels libres et ouverts peuvent contribuer au produit intérieur brut (PIB) de l'Union à hauteur de 65 à 95 milliards d'EUR et peuvent offrir des possibilités notables de croissance à l'économie européenne.*** Afin de ne pas entraver l'innovation ou la recherche, les logiciels libres et ouverts développés ou fournis en dehors du cadre d'une activité commerciale ne devraient pas être couverts par le présent règlement. C'est notamment le cas des logiciels, y compris leurs codes sources et versions modifiées, qui sont librement

logiciel.

partagés et accessibles, utilisables, modifiables et redistribuables. ***L'activité commerciale, au sens de la mise à disposition sur le marché,*** peut ***toutefois*** être caractérisée par le prix facturé pour un ***composant logiciel libre et ouvert***, mais également par ***la monétisation, telle que*** le prix des services d'assistance technique ***ou les mises à jour logicielles payantes, sauf lorsque cela ne sert qu'à récupérer les coûts réels***, par la fourniture d'une plate-forme logicielle par l'intermédiaire de laquelle le fabricant monétise d'autres services, ou par l'utilisation de données à caractère personnel pour des raisons autres qu'aux seules fins d'améliorer la sécurité, la compatibilité ou l'interopérabilité du logiciel. ***Ni le développement collaboratif de composants logiciels libres et ouverts ni leur mise à disposition dans des référentiels ouverts ne devraient constituer une mise sur le marché ou une mise en service. Les circonstances dans lesquelles le produit a été développé ou la manière dont le développement a été financé ne devraient pas être pris en considération au moment de déterminer la nature commerciale ou non commerciale de cette activité. Lorsqu'un logiciel ouvert est intégré dans un produit final comportant des éléments numériques qui est mis sur le marché, l'opérateur économique qui a mis sur le marché le produit final comportant des éléments numériques est responsable de la conformité du produit, y compris des composants libres et ouverts.***

Amendement 7

Proposition de règlement
Considérant 11

Texte proposé par la Commission	*Amendement*
(11) Un internet sécurisé est indispensable au fonctionnement des infrastructures critiques et à la société dans	(11) Un internet sécurisé est indispensable au fonctionnement des infrastructures critiques et à la société dans

son ensemble. La [directive XXX/XXXX (SRI 2)] vise à garantir un niveau élevé de cybersécurité des services fournis par des entités essentielles et importantes, y compris les fournisseurs d'infrastructures numériques qui soutiennent les fonctions essentielles de l'internet ouvert, assurent l'accès à l'internet et les services internet. Il est donc important que les produits comportant des éléments numériques dont les fournisseurs d'infrastructures numériques ont besoin pour assurer le fonctionnement de l'internet soient développés de manière sécurisée et qu'ils respectent les normes de sécurité de l'internet bien établies. Le présent règlement, qui s'applique à tous les matériels et logiciels ***connectables***, vise également à faciliter le respect, par les fournisseurs d'infrastructures numériques, des exigences de la chaîne d'approvisionnement en vertu de la [directive XXX/XXXX (SRI 2)], en veillant à ce que les produits comportant des éléments numériques qu'ils utilisent pour la fourniture de leurs services soient développés de manière sécurisée et à ce qu'ils aient accès à des mises à jour de sécurité en temps utile pour ces produits.

son ensemble. La [directive XXX/XXXX (SRI 2)] vise à garantir un niveau élevé de cybersécurité des services fournis par des entités essentielles et importantes, y compris les fournisseurs d'infrastructures numériques qui soutiennent les fonctions essentielles de l'internet ouvert, assurent l'accès à l'internet et les services internet. Il est donc important que les produits comportant des éléments numériques dont les fournisseurs d'infrastructures numériques ont besoin pour assurer le fonctionnement de l'internet soient développés de manière sécurisée et qu'ils respectent les normes de sécurité de l'internet bien établies. Le présent règlement, qui s'applique à tous les matériels et logiciels ***connectés à un réseau ou dispositif externe***, vise également à faciliter le respect, par les fournisseurs d'infrastructures numériques, des exigences de la chaîne d'approvisionnement en vertu de la [directive XXX/XXXX (SRI 2)], en veillant à ce que les produits comportant des éléments numériques qu'ils utilisent pour la fourniture de leurs services soient développés de manière sécurisée et à ce qu'ils aient accès à des mises à jour de sécurité en temps utile pour ces produits.

Amendement 8

Proposition de règlement
Considérant 15

Texte proposé par la Commission	*Amendement*
(15) Le règlement délégué (UE) 2022/30 précise que les exigences essentielles énoncées à l'article 3, paragraphe 3, point d) (dommages au réseau et mauvaise utilisation des ressources du réseau), point e) (données à caractère personnel et vie privée) et point f) (fraude), de la directive 2014/53/UE s'appliquent à certains équipements radio. La [décision d'exécution (UE) XXX/2022 de la	(15) Le règlement délégué (UE) 2022/30 précise que les exigences essentielles énoncées à l'article 3, paragraphe 3, point d) (dommages au réseau et mauvaise utilisation des ressources du réseau), point e) (données à caractère personnel et vie privée) et point f) (fraude), de la directive 2014/53/UE s'appliquent à certains équipements radio. La [décision d'exécution (UE) XXX/2022 de la

Commission relative à une demande de normalisation adressée aux organisations européennes de normalisation] fixe des exigences pour l'élaboration de normes spécifiques précisant la manière dont ces trois exigences essentielles doivent être traitées. Les exigences essentielles établies par le présent règlement comprennent tous les éléments des exigences essentielles visées à l'article 3, paragraphe 3, points d), e) et f), de la directive 2014/53/UE. En outre, les exigences essentielles énoncées dans le présent règlement sont alignées sur les objectifs des exigences relatives à des normes spécifiques incluses dans cette demande de normalisation. Par conséquent, si la Commission abroge ***ou modifie*** le règlement délégué (UE) 2022/30 de sorte qu'il cesse de s'appliquer à certains produits soumis au présent règlement, la Commission et les organisations européennes de normalisation devraient tenir compte des travaux de normalisation menés dans le cadre de la décision d'exécution C(2022)5637 de la Commission relative à une demande de normalisation du règlement délégué RED [règlement (UE) 2022/30] lors de l'élaboration et du développement de normes harmonisées visant à faciliter la mise en œuvre du présent règlement.

Commission relative à une demande de normalisation adressée aux organisations européennes de normalisation] fixe des exigences pour l'élaboration de normes spécifiques précisant la manière dont ces trois exigences essentielles doivent être traitées. Les exigences essentielles établies par le présent règlement comprennent tous les éléments des exigences essentielles visées à l'article 3, paragraphe 3, points d), e) et f), de la directive 2014/53/UE. En outre, les exigences essentielles énoncées dans le présent règlement sont alignées sur les objectifs des exigences relatives à des normes spécifiques incluses dans cette demande de normalisation. Par conséquent, si la Commission abroge le règlement délégué (UE) 2022/30 de sorte qu'il cesse de s'appliquer à certains produits soumis au présent règlement, la Commission et les organisations européennes de normalisation devraient tenir compte des travaux de normalisation menés dans le cadre de la décision d'exécution C(2022)5637 de la Commission relative à une demande de normalisation du règlement délégué RED [règlement (UE) 2022/30] lors de l'élaboration et du développement de normes harmonisées visant à faciliter la mise en œuvre du présent règlement.

Amendement 9

Proposition de règlement
Considérant 18 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	(18 bis) Afin que les développeurs individuels ou les micro-développeurs de logiciels au sens de la recommandation 2003/361/CE de la Commission ne soient pas confrontés à des obstacles financiers majeurs et ne soient pas dissuadés de tester sur le marché leur preuve de concept ainsi que leur analyse de rentabilisation, ces entités

	devraient être tenues de faire tout ce qui est en leur pouvoir pour se conformer aux exigences de la présente proposition dans les six mois suivant la mise sur le marché d'un logiciel. Ce régime spécial devrait permettre d'éviter l'effet dissuasif que les coûts de conformité et d'accès élevés pourraient avoir sur les entrepreneurs ou les personnes qualifiées qui envisagent de développer des logiciels dans l'Union. Toutefois, ce régime spécial ne devrait pas s'appliquer aux produits hautement critiques comportant des éléments numériques.

Amendement 10

Proposition de règlement
Considérant 19

Texte proposé par la Commission	*Amendement*
(19) Certaines tâches prévues par le présent règlement devraient être exécutées par l'ENISA, conformément à l'article 3, paragraphe 2, du règlement (UE) 2019/881. L'ENISA devrait notamment recevoir des ***notifications*** des ***fabricants*** concernant les vulnérabilités activement exploitées des produits comportant des éléments numériques ainsi que les incidents ayant une incidence sur la sécurité de ces produits. L'ENISA devrait également transmettre ces notifications aux centres de réponse aux incidents de sécurité informatique (CSIRT) concernés ou, respectivement, aux points de contact uniques pertinents des États membres désignés conformément à l'article [article X] de la directive [directive XXX/XXXX (SRI 2)], et informer les autorités de surveillance du marché concernées de ***la*** vulnérabilité notifiée. Sur la base des informations qu'elle recueille, l'ENISA devrait préparer un rapport technique bisannuel sur les tendances émergentes concernant les risques de cybersécurité dans les produits	(19) Certaines tâches prévues par le présent règlement devraient être exécutées par l'ENISA, conformément à l'article 3, paragraphe 2, du règlement (UE) 2019/881. L'ENISA devrait notamment recevoir des ***fabricants, sous la forme d'une alerte précoce,*** des ***notifications*** concernant les vulnérabilités activement exploitées des produits comportant des éléments numériques ainsi que les incidents ayant une incidence ***importante*** sur la sécurité de ces produits. L'ENISA devrait également transmettre ces notifications aux centres de réponse aux incidents de sécurité informatique (CSIRT) concernés ou, respectivement, aux points de contact uniques pertinents des États membres désignés conformément à l'article [article X] de la directive [directive XXX/XXXX (SRI 2)], et informer ***immédiatement*** les autorités de surveillance du marché concernées de ***l'existence d'une vulnérabilité et, le cas échéant, des mesures d'atténuation du risque potentiel. En l'absence de mesure corrective ou d'atténuation pour une***

comportant des éléments numériques et le soumettre au groupe de coopération visé dans la directive [directive XXX/XXXX (SRI 2)]. En outre, eu égard à son expertise et à son mandat, l'ENISA devrait être en mesure de soutenir le processus de mise en œuvre du présent règlement. Elle devrait notamment pouvoir proposer des activités conjointes à mener par les autorités de surveillance du marché sur la base d'indications ou d'informations concernant une non-conformité potentielle au présent règlement, dans plusieurs États membres, de produits comportant des éléments numériques ou recenser les catégories de produits pour lesquelles des actions de contrôle coordonnées simultanées devraient être organisées. Dans des circonstances exceptionnelles, à la demande de la Commission, l'ENISA devrait être en mesure de procéder à des évaluations portant sur des produits comportant des éléments numériques spécifiques qui présentent un risque de cybersécurité important, lorsqu'une intervention immédiate est nécessaire pour préserver le bon fonctionnement du marché intérieur.

vulnérabilité notifiée***, l'ENISA devrait veiller à ce que les informations concernant ladite vulnérabilité notifiée soient partagées conformément à des protocoles de sécurité stricts et selon le principe du besoin d'en connaître***. Sur la base des informations qu'elle recueille, l'ENISA devrait préparer un rapport technique bisannuel sur les tendances émergentes concernant les risques de cybersécurité dans les produits comportant des éléments numériques et le soumettre au groupe de coopération visé dans la directive [directive XXX/XXXX (SRI 2)]. En outre, eu égard à son expertise et à son mandat, l'ENISA devrait être en mesure de soutenir le processus de mise en œuvre du présent règlement. Elle devrait notamment pouvoir proposer des activités conjointes à mener par les autorités de surveillance du marché sur la base d'indications ou d'informations concernant une non-conformité potentielle au présent règlement, dans plusieurs États membres, de produits comportant des éléments numériques ou recenser les catégories de produits pour lesquelles des actions de contrôle coordonnées simultanées devraient être organisées. Dans des circonstances exceptionnelles, à la demande de la Commission, l'ENISA devrait être en mesure de procéder à des évaluations portant sur des produits comportant des éléments numériques spécifiques qui présentent un risque de cybersécurité important, lorsqu'une intervention immédiate est nécessaire pour préserver le bon fonctionnement du marché intérieur.

Amendement 11

Proposition de règlement
Considérant 20

Texte proposé par la Commission	*Amendement*
(20) Le marquage CE devrait être	(20) Le marquage CE devrait être

apposé sur les produits comportant des éléments numériques pour indiquer leur conformité avec le présent règlement, afin qu'ils puissent circuler librement dans le marché intérieur. Les États membres devraient s'abstenir de créer des entraves injustifiées à la mise sur le marché de produits comportant des éléments numériques qui satisfont aux exigences fixées dans le présent règlement et portent le marquage CE.

apposé sur les produits comportant des éléments numériques pour indiquer ***de manière visible, lisible et indélébile*** leur conformité avec le présent règlement, afin qu'ils puissent circuler librement dans le marché intérieur. Les États membres devraient s'abstenir de créer des entraves injustifiées à la mise sur le marché de produits comportant des éléments numériques qui satisfont aux exigences fixées dans le présent règlement et portent le marquage CE.

Amendement 12

Proposition de règlement
Considérant 22

Texte proposé par la Commission	*Amendement*
(22) Afin de garantir que les produits comportant des éléments numériques, lorsqu'ils sont mis sur le marché, ne présentent pas de risques de cybersécurité pour les personnes et les organisations, il convient de fixer des exigences essentielles pour ces produits. Lorsque ces produits sont modifiés ultérieurement, par des moyens physiques ou numériques, d'une manière qui n'est pas prévue par le fabricant et qui peut impliquer qu'ils ne satisfont plus aux exigences essentielles pertinentes, la modification devrait être considérée comme substantielle. Par exemple, les mises à jour de logiciels ou les réparations pourraient être assimilées à des opérations d'entretien pour autant qu'elles ne modifient pas un produit déjà mis sur le marché d'une manière qui soit susceptible d'en compromettre la conformité aux exigences applicables ou de modifier l'utilisation prévue pour laquelle le produit a été évalué. Comme c'est le cas pour les réparations ou modifications physiques, un produit comportant des éléments numériques doit être considéré comme substantiellement modifié par une modification logicielle lorsque la mise à	(22) Afin de garantir que les produits comportant des éléments numériques, lorsqu'ils sont mis sur le marché, ne présentent pas de risques de cybersécurité pour les personnes et les organisations, il convient de fixer des exigences essentielles pour ces produits. Lorsque ces produits sont modifiés ultérieurement, par des moyens physiques ou numériques, d'une manière qui n'est pas prévue par le fabricant et qui peut impliquer qu'ils ne satisfont plus aux exigences essentielles pertinentes, la modification devrait être considérée comme substantielle. Par exemple, les mises à jour de logiciels ou les réparations***, telles qu'une modification mineure du code source de nature à améliorer la sécurité et le fonctionnement,*** pourraient être assimilées à des opérations d'entretien pour autant qu'elles ne modifient pas un produit déjà mis sur le marché d'une manière qui soit susceptible d'en compromettre la conformité aux exigences applicables ou de modifier l'utilisation prévue pour laquelle le produit a été évalué. Comme c'est le cas pour les réparations ou modifications physiques, un produit comportant des éléments

jour du logiciel modifie les fonctions, le type ou les performances initialement prévues du produit et que ces modifications n'ont pas été prévues dans l'évaluation initiale des risques, ou lorsque la nature du danger a changé ou que le niveau de risque a augmenté en raison de la mise à jour du logiciel.

numériques doit être considéré comme substantiellement modifié par une modification logicielle lorsque la mise à jour du logiciel modifie les fonctions, le type ou les performances initialement prévues du produit et que ces modifications n'ont pas été prévues dans l'évaluation initiale des risques, ou lorsque la nature du danger a changé ou que le niveau de risque a augmenté en raison de la mise à jour du logiciel.

Amendement 13

Proposition de règlement
Considérant 23

Texte proposé par la Commission	*Amendement*
(23) Conformément à la notion généralement établie de modification substantielle pour les produits régis par la législation d'harmonisation de l'Union, chaque fois que se produit une modification substantielle de nature à affecter la conformité d'un produit au présent règlement ou lorsque l'utilisation prévue de ce produit change, il convient de vérifier la conformité du produit comportant des éléments numériques et, le cas échéant, de ***le soumettre*** à ***une nouvelle évaluation*** de la conformité. Le cas échéant, si le fabricant a recours à une évaluation de la conformité faisant intervenir un tiers, les modifications susceptibles d'entraîner des modifications substantielles devraient être notifiées à ce dernier.	(23) Conformément à la notion généralement établie de modification substantielle pour les produits régis par la législation d'harmonisation de l'Union, chaque fois que se produit une modification substantielle de nature à affecter la conformité d'un produit au présent règlement ou lorsque l'utilisation prévue de ce produit change, il convient de vérifier la conformité du produit comportant des éléments numériques et, le cas échéant, de ***mettre*** à ***jour l'évaluation*** de la conformité. Le cas échéant, si le fabricant a recours à une évaluation de la conformité faisant intervenir un tiers, les modifications susceptibles d'entraîner des modifications substantielles devraient être notifiées à ce dernier. ***L'évaluation ultérieure de la conformité devrait porter sur les modifications ayant conduit à la nouvelle évaluation, à moins que ces modifications n'aient une incidence importante sur la conformité d'autres parties du produit. Lorsqu'une mise à jour logicielle est effectuée, le fabricant ne devrait pas être tenu de procéder à une autre évaluation de la conformité du produit comportant des éléments numériques, sauf si la mise à jour***

logicielle entraîne une modification substantielle du produit comportant des éléments numériques.

Amendement 14

Proposition de règlement
Considérant 24 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	(24 bis) Les fabricants de produits comportant des éléments numériques devraient veiller à ce que les mises à jour des logiciels soient fournies de manière claire et transparente et à ce qu'une distinction claire soit établie entre les mises à jour de sécurité et les mises à jour de fonctionnalités. Si les mises à jour de sécurité visent à diminuer le niveau de risque d'un produit comportant des éléments numériques, l'application des mises à jour de fonctionnalités fournies par le fabricant devrait toujours rester à la discrétion de l'utilisateur. Les fabricants devraient donc fournir ces mises à jour séparément, sauf si cela n'est pas possible d'un point de vue technique. Les fabricants devraient fournir aux consommateurs des informations pertinentes sur les motifs de chaque mise à jour et sur l'incidence prévue de celle-ci sur le produit, ainsi qu'un mécanisme de renonciation clair et facile à utiliser.

Amendement 15

Proposition de règlement
Considérant 25

Texte proposé par la Commission	*Amendement*
(25) Les produits comportant des éléments numériques devraient être considérés comme critiques si l'exploitation de vulnérabilités potentielles	(25) Les produits comportant des éléments numériques devraient être considérés comme critiques si l'exploitation de vulnérabilités potentielles

de cybersécurité dans ces produits peut avoir de graves répercussions en raison, entre autres, de la fonctionnalité liée à la cybersécurité ou de l'utilisation prévue. En particulier, les vulnérabilités de produits comportant des éléments numériques qui ont une fonctionnalité liée à la cybersécurité, tels que les éléments sécurisés, peuvent provoquer une propagation des problèmes de sécurité tout au long de la chaîne d'approvisionnement. La gravité des effets d'un incident de cybersécurité peut également augmenter ***selon*** l'utilisation prévue du produit***, par exemple s'il est employé dans un cadre industriel*** ou dans le contexte d'une entité essentielle du type visé à l'annexe [annexe I] de la directive [directive XXX/XXXX (SRI 2)], ou pour l'exécution de fonctions critiques ou sensibles, telles que le traitement de données à caractère personnel.

de cybersécurité dans ces produits peut avoir de graves répercussions en raison, entre autres, de la fonctionnalité liée à la cybersécurité ou de l'utilisation prévue. En particulier, les vulnérabilités de produits comportant des éléments numériques qui ont une fonctionnalité liée à la cybersécurité, tels que les éléments sécurisés, peuvent provoquer une propagation des problèmes de sécurité tout au long de la chaîne d'approvisionnement. La gravité des effets d'un incident de cybersécurité peut également augmenter ***en considération de*** l'utilisation prévue du produit ***dans des applications critiques au sein d'environnements sensibles*** ou dans le contexte d'une entité essentielle du type visé à l'annexe [annexe I] de la directive [directive XXX/XXXX (SRI 2)], ou pour l'exécution de fonctions critiques ou sensibles, telles que le traitement de données à caractère personnel.

Amendement 16

Proposition de règlement
Considérant 26

Texte proposé par la Commission	*Amendement*
(26) Les produits critiques comportant des éléments numériques devraient être soumis à des procédures d'évaluation de la conformité plus strictes, tout en conservant une approche proportionnée. À cette fin, les produits critiques comportant des éléments numériques devraient être divisés en deux catégories, reflétant le niveau de risque de cybersécurité lié à ces catégories de produits. Un cyberincident potentiel impliquant des produits de classe II pourrait avoir des conséquences négatives plus importantes qu'un incident impliquant des produits de classe I, par exemple en raison de la nature de leur fonction liée à la cybersécurité ou de leur utilisation prévue dans des environnements sensibles, et ces produits devraient donc faire l'objet d'une	(26) Les produits critiques comportant des éléments numériques devraient être soumis à des procédures d'évaluation de la conformité plus strictes, tout en conservant une approche proportionnée. À cette fin, les produits critiques comportant des éléments numériques devraient être divisés en deux catégories, reflétant le niveau de risque de cybersécurité lié à ces catégories de produits. Un cyberincident potentiel impliquant des produits de classe II pourrait avoir des conséquences négatives plus importantes qu'un incident impliquant des produits de classe I, par exemple en raison de la nature de leur fonction liée à la cybersécurité ou de leur utilisation prévue dans des environnements sensibles, et ces produits devraient donc faire l'objet d'une

procédure d'évaluation de la conformité plus stricte.

procédure d'évaluation de la conformité plus stricte. ***À titre d'exception, les petites entreprises et les microentreprises devraient pouvoir employer la procédure applicable aux produits de classe I.***

Amendement 17

Proposition de règlement
Considérant 29

Texte proposé par la Commission	*Amendement*
(29) Les produits comportant des éléments numériques classés comme systèmes d'IA à haut risque conformément à l'article 6 du règlement[27] [règlement sur l'IA] qui relèvent du champ d'application du présent règlement devraient satisfaire aux exigences essentielles énoncées dans celui-ci. Lorsque ces systèmes d'IA à haut risque satisfont aux exigences essentielles du présent règlement, ils devraient être réputés conformes aux exigences en matière de cybersécurité énoncées à l'article [article 15] du règlement [règlement sur l'IA], dans la mesure où ces exigences sont couvertes par la déclaration UE de conformité, ou par certaines parties de celle-ci, délivrée en vertu du présent règlement. S'agissant des procédures d'évaluation de la conformité relatives aux exigences essentielles de cybersécurité d'un produit comportant des éléments numériques couvert par le présent règlement et classé comme système d'IA à haut risque, les dispositions pertinentes ***de l'article 43*** du règlement [règlement sur l'IA] devraient de manière générale s'appliquer en lieu et place des dispositions correspondantes du présent règlement. ***Toutefois,*** l'application de cette règle ***ne*** devrait ***pas entraîner de réduction du*** niveau ***d'assurance nécessaire*** pour les produits critiques comportant des éléments numériques couverts par le présent règlement. ***Par conséquent, par dérogation à cette règle,*** les systèmes d'IA	(29) Les produits comportant des éléments numériques ***ou les quasi-produits comportant des éléments numériques*** classés comme systèmes d'IA à haut risque conformément à l'article 6 du règlement[27] [règlement sur l'IA] qui relèvent du champ d'application du présent règlement devraient satisfaire aux exigences essentielles énoncées dans celui-ci. Lorsque ces systèmes d'IA à haut risque satisfont aux exigences essentielles du présent règlement, ils devraient être réputés conformes aux exigences en matière de cybersécurité énoncées à l'article [article 15] du règlement [règlement sur l'IA], dans la mesure où ces exigences sont couvertes par la déclaration UE de conformité, ou par certaines parties de celle-ci, délivrée en vertu du présent règlement. S'agissant des procédures d'évaluation de la conformité relatives aux exigences essentielles de cybersécurité d'un produit comportant des éléments numériques couvert par le présent règlement et classé comme système d'IA à haut risque, les dispositions pertinentes ***[des dispositions applicables]*** du règlement [règlement sur l'IA] devraient de manière générale s'appliquer en lieu et place des dispositions correspondantes du présent règlement. L'application de cette règle devrait ***créer un*** niveau ***élevé d'assurance*** pour les produits critiques comportant des éléments numériques couverts par le présent règlement. ***Pour*** les systèmes d'IA

à haut risque qui relèvent du champ d'application du règlement [règlement sur l'IA] et sont également considérés comme des produits critiques comportant des éléments numériques ***en vertu*** du présent règlement ***et auxquels s'applique la procédure d'évaluation*** de la ***conformité fondée sur le contrôle interne visée à l'annexe VI du règlement [règlement sur l'IA] devraient être soumis aux dispositions*** du présent règlement ***relatives à l'évaluation de*** la ***conformité en ce qui concerne les exigences essentielles énoncées dans celui-ci. Dans*** ce ***cas, pour tous*** les ***autres aspects couverts par le règlement [règlement sur l'IA], les dispositions correspondantes relatives à l'évaluation*** de la conformité ***fondée sur le contrôle interne énoncées*** à ***l'annexe VI du règlement [règlement sur IA] devraient s'appliquer***.	à haut risque qui relèvent du champ d'application du règlement [règlement sur l'IA] et sont également considérés comme des produits critiques comportant des éléments numériques ***au titre*** du présent règlement***, l'organisme sectoriel notifié responsable devrait être chargé*** de la ***réalisation de l'évaluation de la conformité en application*** du présent règlement ***et diriger*** la ***procédure administrative de façon à*** ce ***que*** les ***opérateurs économiques puissent adresser leur demande d'évaluation*** de la conformité à ***un organisme réglementaire unique***.
[27] Règlement [le règlement sur l'IA].	[27] Règlement [le règlement sur l'IA].

Amendement 18

Proposition de règlement
Considérant 32

Texte proposé par la Commission	*Amendement*
(32) Afin de garantir la sécurité des produits comportant des éléments numériques au moment de leur mise sur le marché et tout au long de leur cycle de vie, il est nécessaire de définir des exigences essentielles en matière de gestion de la vulnérabilité et des exigences essentielles en matière de cybersécurité concernant les propriétés des produits comportant des éléments numériques. Les fabricants devraient se conformer à toutes les exigences essentielles liées à la gestion des vulnérabilités et veiller à ce que tous leurs produits soient livrés sans aucune vulnérabilité exploitable connue, mais ils devraient en outre déterminer les autres	(32) Afin de garantir la sécurité des produits comportant des éléments numériques au moment de leur mise sur le marché et tout au long de leur cycle de vie, il est nécessaire de définir des exigences essentielles en matière de gestion de la vulnérabilité et des exigences essentielles en matière de cybersécurité concernant les propriétés des produits comportant des éléments numériques. Les fabricants devraient se conformer à toutes les exigences essentielles liées à la gestion des vulnérabilités et veiller à ce que tous leurs produits soient livrés sans aucune vulnérabilité exploitable connue, mais ils devraient en outre déterminer les autres

exigences essentielles liées aux propriétés du produit pertinentes pour le type de produit concerné. À cette fin, les fabricants devraient entreprendre une évaluation des risques de cybersécurité associés à un produit comportant des éléments numériques afin de recenser les risques et les exigences essentielles pertinents et d'appliquer de manière appropriée des normes harmonisées ***ou des spécifications communes*** appropriées.

exigences essentielles liées aux propriétés du produit pertinentes pour le type de produit concerné. À cette fin, les fabricants devraient entreprendre une évaluation des risques de cybersécurité associés à un produit comportant des éléments numériques afin de recenser les risques et les exigences essentielles pertinents et d'appliquer de manière appropriée des normes harmonisées appropriées.

Amendement 19

Proposition de règlement
Considérant 33 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	(33 bis) Pour garantir que les produits sont conçus, développés et fabriqués conformément aux exigences essentielles prévues à l'annexe I, section 1, les fabricants devraient faire preuve de diligence raisonnable lors de l'intégration de composants provenant de tiers dans des produits comportant des éléments numériques. Tel est le cas des composants qui sont adaptés au produit et y sont intégrés en tenant compte de ses spécificités, en particulier pour ce qui est des logiciels libres et ouverts qui n'ont pas été mis sur le marché moyennant une monétisation, financière ou autre.

Amendement 20

Proposition de règlement
Considérant 34

Texte proposé par la Commission	*Amendement*
(34) Afin de garantir que les CSIRT nationaux et le guichet unique désigné conformément à l'article [article X] de la directive [directive XX/XXXX (SRI 2)]	(34) Afin de garantir que les CSIRT nationaux et le guichet unique désigné conformément à l'article [article X] de la directive [directive XX/XXXX (SRI 2)]

reçoivent les informations nécessaires à l'accomplissement de leurs tâches et à l'élévation du niveau global de cybersécurité des entités essentielles et importantes, et afin de garantir le fonctionnement efficace des autorités de surveillance du marché, les fabricants de produits comportant des éléments numériques devraient notifier à l'ENISA les vulnérabilités activement exploitées. Étant donné que la plupart des produits comportant des éléments numériques sont commercialisés sur l'ensemble du marché intérieur, toute vulnérabilité exploitée dans un de ces produits devrait être considérée comme une menace pour le fonctionnement du marché intérieur. Les fabricants devraient également envisager de communiquer les vulnérabilités fixes à la base de données européenne sur les vulnérabilités établie en vertu de la directive [directive XX/XXXX (SRI 2)] et gérée par l'ENISA ou à toute autre base de données sur les vulnérabilités accessible au public.

reçoivent les informations nécessaires à l'accomplissement de leurs tâches et à l'élévation du niveau global de cybersécurité des entités essentielles et importantes, et afin de garantir le fonctionnement efficace des autorités de surveillance du marché, les fabricants de produits comportant des éléments numériques devraient notifier à l'ENISA***, dans les meilleurs délais et en tout état de cause 48 heures au plus tard après en avoir eu connaissance, au moyen d'une alerte précoce,*** les vulnérabilités activement exploitées***. Les fabricants devraient, dans les meilleurs délais après avoir eu connaissance de vulnérabilités activement exploitées ayant une incidence importante sur la sécurité du produit comportant des éléments numériques, communiquer à l'ENISA des précisions supplémentaires sur ladite vulnérabilité exploitée. Toute autre vulnérabilité n'ayant pas d'incidence importante sur la sécurité du produit comportant des éléments numériques devrait être signalée à l'ENISA une fois traitée***. Étant donné que la plupart des produits comportant des éléments numériques sont commercialisés sur l'ensemble du marché intérieur, toute vulnérabilité exploitée dans un de ces produits devrait être considérée comme une menace pour le fonctionnement du marché intérieur. Les fabricants devraient également envisager de communiquer les vulnérabilités fixes à la base de données européenne sur les vulnérabilités établie en vertu de la directive [directive XX/XXXX (SRI 2)] et gérée par l'ENISA ou à toute autre base de données sur les vulnérabilités accessible au public.

Amendement 21

Proposition de règlement
Considérant 34 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	(34 bis) L'ENISA devrait être responsable de la publication et de la tenue à jour d'une base de données des vulnérabilités exploitées connues. Les fabricants devraient assurer une veille de la base de données et communiquer les vulnérabilités constatées dans leurs produits.

Amendement 22

Proposition de règlement
Considérant 35

Texte proposé par la Commission	*Amendement*
(35) Les fabricants devraient également signaler à l'ENISA tout incident ayant des répercussions sur la sécurité du produit comportant des éléments numériques. Nonobstant les obligations de signalement d'incidents prévues par la directive [directive XXX/XXXX (SRI 2)] pour les entités essentielles et importantes, il est essentiel que l'ENISA, les guichets uniques désignés par les États membres conformément à l'article [article X] de la directive [directive XXX/XXXX (SRI 2)] et les autorités de surveillance du marché reçoivent des informations des fabricants de produits comportant des éléments numériques leur permettant d'évaluer la sécurité de ces produits. Afin de garantir que les utilisateurs puissent réagir rapidement aux incidents ayant un impact sur la sécurité de leurs produits comportant des éléments numériques, les fabricants devraient également informer leurs utilisateurs de tout incident de ce type et, le cas échéant, de toute mesure corrective que les utilisateurs peuvent mettre en œuvre pour atténuer l'impact de l'incident, par exemple en publiant des informations pertinentes sur leur site internet ou, lorsque le fabricant est en mesure de contacter les	(35) Les fabricants devraient également signaler à l'ENISA***, au moyen d'une alerte précoce,*** tout incident ayant des répercussions ***importantes*** sur la sécurité du produit comportant des éléments numériques. ***Les fabricants devraient communiquer à l'ENISA, dans les meilleurs délais et en tout état de cause dans les 72 heures après avoir eu connaissance de l'incident important relatif au produit comportant des éléments numériques, des précisions supplémentaires sur ledit incident important.*** Nonobstant les obligations de signalement d'incidents prévues par la directive [directive XXX/XXXX (SRI 2)] pour les entités essentielles et importantes, il est essentiel que l'ENISA, les guichets uniques désignés par les États membres conformément à l'article [article X] de la directive [directive XXX/XXXX (SRI 2)] et les autorités de surveillance du marché reçoivent des informations des fabricants de produits comportant des éléments numériques leur permettant d'évaluer la sécurité de ces produits. Afin de garantir que les utilisateurs puissent réagir rapidement aux incidents ayant un impact ***important*** sur la sécurité de leurs produits

utilisateurs et lorsque les risques le justifient, en contactant directement les utilisateurs.	comportant des éléments numériques, les fabricants devraient également informer leurs utilisateurs de tout incident de ce type***, s'il y a lieu et si celui-ci risque de leur nuire,*** et, le cas échéant, de toute ***mesure d'atténuation des risques ou*** mesure corrective que les utilisateurs peuvent mettre en œuvre pour atténuer l'impact de l'incident ***important***, par exemple en publiant des informations pertinentes sur leur site internet ou, lorsque le fabricant est en mesure de contacter les utilisateurs et lorsque les risques le justifient, en contactant directement les utilisateurs. ***Sans préjudice d'autres obligations, les fabricants qui décèlent une vulnérabilité dans un composant intégré à un produit comportant des éléments numériques, y compris dans un composant libre et ouvert, devraient signaler la vulnérabilité à la personne ou à l'entité qui assure l'entretien du composant, ainsi que les mesures correctives prises.***

Amendement 23

Proposition de règlement
Considérant 37 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	(37 bis) Aux termes de l'accord de l'Organisation mondiale du commerce (OMC) sur les obstacles techniques au commerce, dans les cas où des règlements techniques sont requis et où des normes internationales pertinentes existent, les membres de l'OMC devraient utiliser ces normes comme base de leurs propres règlements techniques. Il importe d'éviter tout chevauchement d'activité entre les organisations de normalisation, les normes internationales visant à faciliter l'harmonisation des règlements et normes techniques nationaux et régionaux et, ce faisant, à réduire les obstacles techniques non tarifaires au commerce. La

cybersécurité étant un problème mondial, l'Union devrait s'efforcer de parvenir à un alignement maximal. Pour atteindre cet objectif, la demande de normalisation effectuée pour le présent règlement en application de l'article 10 du règlement 1025/2012 devrait tendre à réduire les obstacles à l'acceptation des normes en publiant leurs références au Journal officiel de l'Union, conformément à l'article 10, paragraphe 6, du règlement 1025/2012.

Amendement 24

Proposition de règlement
Considérant 37 ter (nouveau)

Texte proposé par la Commission	*Amendement*
	(37 ter) Compte tenu de l'étendue du champ d'application du présent règlement, l'élaboration en temps utile de normes harmonisées représente un défi de taille. Pour renforcer au plus vite la sécurité des produits comportant des éléments numériques sur le marché de l'Union, la Commission devrait être habilitée, pendant une durée limitée, à déclarer que les normes internationales existantes en matière de cybersécurité des produits satisfont aux exigences du présent règlement. Ces normes devraient être publiées en tant que normes conférant une présomption de conformité.

Amendement 25

Proposition de règlement
Considérant 38

Texte proposé par la Commission	*Amendement*
(38) Afin de faciliter l'évaluation de la conformité aux exigences établies par le présent règlement, il convient de prévoir	(38) Afin de faciliter l'évaluation de la conformité aux exigences établies par le présent règlement, il convient de prévoir

une présomption de conformité pour les produits dont les éléments numériques sont conformes à des normes harmonisées, qui traduisent les exigences essentielles du présent règlement en spécifications techniques détaillées et sont adoptées conformément au règlement (UE) nº 1025/2012 du Parlement européen et du Conseil[29]. Le règlement (UE) nº 1025/2012 prévoit une procédure pour la formulation d'objections à l'encontre de normes harmonisées lorsque celles-ci ne satisfont pas pleinement aux exigences du présent règlement.

[29] Règlement (UE) nº 1025/2012 du Parlement européen et du Conseil du 25 octobre 2012 relatif à la normalisation européenne, modifiant les directives 89/686/CEE et 93/15/CEE du Conseil ainsi que les directives 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE et 2009/105/CE du Parlement européen et du Conseil et abrogeant la décision 87/95/CEE du Conseil et la décision nº 1673/2006/CE du Parlement européen et du Conseil (JO L 316 du 14.11.2012, p. 12).

une présomption de conformité pour les produits dont les éléments numériques sont conformes à des normes harmonisées, qui traduisent les exigences essentielles du présent règlement en spécifications techniques détaillées et sont adoptées conformément au règlement (UE) nº 1025/2012 du Parlement européen et du Conseil[29]. Le règlement (UE) nº 1025/2012 prévoit une procédure pour la formulation d'objections à l'encontre de normes harmonisées lorsque celles-ci ne satisfont pas pleinement aux exigences du présent règlement. ***Le processus de normalisation devrait garantir une représentation équilibrée des intérêts et la participation effective des parties prenantes de la société civile, y compris des organisations de consommateurs.***

[29] Règlement (UE) nº 1025/2012 du Parlement européen et du Conseil du 25 octobre 2012 relatif à la normalisation européenne, modifiant les directives 89/686/CEE et 93/15/CEE du Conseil ainsi que les directives 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE et 2009/105/CE du Parlement européen et du Conseil et abrogeant la décision 87/95/CEE du Conseil et la décision nº 1673/2006/CE du Parlement européen et du Conseil (JO L 316 du 14.11.2012, p. 12).

Amendement 26

Proposition de règlement
Considérant 41

Texte proposé par la Commission	*Amendement*
(41) ***En l'absence de*** normes harmonisées ***ou lorsque les normes harmonisées ne répondent*** pas ***suffisamment aux exigences essentielles du présent règlement***, la Commission devrait pouvoir adopter des spécifications	(41) ***Lorsqu'aucune référence à des*** normes harmonisées ***couvrant les exigences énoncées à l'annexe I n'a été publiée au Journal officiel de l'Union européenne conformément au règlement (UE) nº1025/2012 et qu'il***

communes au moyen d'actes d'exécution. Les raisons de l'élaboration de telles spécifications communes, en lieu et place de normes harmonisées, pourraient inclure un refus de la demande de normalisation par l'une des organisations européennes de normalisation, des retards indus dans la mise en place de normes harmonisées appropriées ou un non-respect des exigences du présent règlement ou d'une demande de la Commission. Afin de faciliter l'évaluation de la conformité aux exigences essentielles prévues par le présent règlement, il convient d'établir une présomption de conformité pour les produits comportant des éléments numériques répondant aux spécifications communes adoptées par la Commission en vertu du présent règlement, aux fins de l'expression de spécifications techniques détaillées sur la base de ces exigences.

n'est pas ***prévu que la publication d'une telle référence intervienne dans un délai raisonnable***, la Commission devrait pouvoir adopter des spécifications communes au moyen d'actes d'exécution. Les raisons de l'élaboration de telles spécifications communes, en lieu et place de normes harmonisées, pourraient inclure un refus de la demande de normalisation par l'une des organisations européennes de normalisation, des retards indus dans la mise en place de normes harmonisées appropriées ou un non-respect des exigences du présent règlement ou d'une demande de la Commission. Afin de faciliter l'évaluation de la conformité aux exigences essentielles prévues par le présent règlement, il convient d'établir une présomption de conformité pour les produits comportant des éléments numériques répondant aux spécifications communes adoptées par la Commission en vertu du présent règlement, aux fins de l'expression de spécifications techniques détaillées sur la base de ces exigences.

Amendement 27

Proposition de règlement
Considérant 43

Texte proposé par la Commission	*Amendement*
(43) Le marquage CE, qui matérialise la conformité d'un produit, est le résultat visible de tout un processus englobant l'évaluation de conformité au sens large. Le règlement (CE) nº 765/2008 du Parlement européen et du Conseil[30] établit les principes généraux régissant le marquage CE. Les règles régissant l'apposition du marquage CE sur les produits comportant des éléments numériques devraient être définies par le présent règlement. Le marquage CE devrait être le seul marquage garantissant la conformité d'un produit comportant des éléments numériques aux exigences du	(43) Le marquage CE, qui matérialise la conformité d'un produit, est le résultat visible de tout un processus englobant l'évaluation de conformité au sens large. Le règlement (CE) nº 765/2008 du Parlement européen et du Conseil[30] établit les principes généraux régissant le marquage CE. Les règles régissant l'apposition du marquage CE sur les produits comportant des éléments numériques devraient être définies par le présent règlement. Le marquage CE devrait être le seul marquage garantissant la conformité d'un produit comportant des éléments numériques aux exigences du

présent règlement.	présent règlement. ***Toutefois, un quasi-produit comportant des éléments numériques ne porte pas le marquage CE prévu par le présent règlement, sans préjudice des dispositions de marquage qui résultent de toute autre disposition législative de l'Union applicable. En ce qui concerne les quasi-produits comportant des éléments numériques, les fabricants établissent une déclaration UE d'incorporation.***
[30] Règlement (CE) nº 765/2008 du Parlement européen et du Conseil du 9 juillet 2008 fixant les prescriptions relatives à l'accréditation et abrogeant le règlement (CEE) nº 339/93 (JO L 218 du 13.8.2008, p. 30).	[30] Règlement (CE) nº 765/2008 du Parlement européen et du Conseil du 9 juillet 2008 fixant les prescriptions relatives à l'accréditation et abrogeant le règlement (CEE) nº 339/93 (JO L 218 du 13.8.2008, p. 30).

Amendement 28

Proposition de règlement
Considérant 45

Texte proposé par la Commission	*Amendement*
(45) En règle générale, l'évaluation de la conformité des produits comportant des éléments numériques ***devrait*** être effectuée par le fabricant sous sa propre responsabilité, conformément à la procédure fondée sur le module A de la décision 768/2008/CE. Le fabricant devrait conserver la possibilité de choisir une procédure d'évaluation de la conformité plus stricte faisant intervenir un tiers. Si le produit est classé comme produit critique de classe I, une assurance supplémentaire est requise pour démontrer la conformité aux exigences essentielles énoncées dans le présent règlement. Le fabricant devrait appliquer des normes harmonisées***, des spécifications communes*** ou des schémas de certification de cybersécurité au titre du règlement (UE) 2019/881, répertoriés par la Commission dans un acte d'exécution, s'il souhaite effectuer l'évaluation de la	(45) En règle générale, ***les exigences relatives à*** l'évaluation de la conformité des produits comportant des éléments numériques ***devraient être fondées sur les risques et, à cet égard, l'évaluation pourrait, dans de nombreux cas,*** être effectuée par le fabricant sous sa propre responsabilité, conformément à la procédure fondée sur le module A de la décision 768/2008/CE. Le fabricant devrait conserver la possibilité de choisir une procédure d'évaluation de la conformité plus stricte faisant intervenir un tiers. Si le produit est classé comme produit critique de classe I, une assurance supplémentaire est requise pour démontrer la conformité aux exigences essentielles énoncées dans le présent règlement. Le fabricant devrait appliquer des normes harmonisées ou des schémas de certification de cybersécurité au titre du règlement (UE) 2019/881,

conformité sous sa propre responsabilité (module A). Si le fabricant n'applique pas ces normes harmonisées***, spécifications communes*** ou schémas de certification de cybersécurité, il devrait se soumettre à une évaluation de la conformité par un tiers. Compte tenu de la charge administrative pesant sur les fabricants et du fait que la cybersécurité joue un rôle important dans la phase de conception et de développement des produits matériels et immatériels comportant des éléments numériques, les procédures d'évaluation de la conformité fondées respectivement sur les modules B+C ou H de la décision 768/2008/CE ont été retenues comme étant les plus appropriées pour évaluer de manière proportionnée et efficace la conformité des produits critiques comportant des éléments numériques. Le fabricant qui fait procéder à l'évaluation de conformité par un tiers peut choisir la procédure qui convient le mieux à son processus de conception et de production. Compte tenu du risque de cybersécurité encore plus grand lié à l'utilisation de produits classés comme produits critiques de classe II, l'évaluation de la conformité de ces produits devrait toujours prévoir l'intervention d'un tiers.

répertoriés par la Commission dans un acte d'exécution, s'il souhaite effectuer l'évaluation de la conformité sous sa propre responsabilité (module A). Si le fabricant n'applique pas ces normes harmonisées ou schémas de certification de cybersécurité, il devrait se soumettre à une évaluation de la conformité par un tiers. Compte tenu de la charge administrative pesant sur les fabricants et du fait que la cybersécurité joue un rôle important dans la phase de conception et de développement des produits matériels et immatériels comportant des éléments numériques, les procédures d'évaluation de la conformité fondées respectivement sur les modules B+C ou H de la décision 768/2008/CE ont été retenues comme étant les plus appropriées pour évaluer de manière proportionnée et efficace la conformité des produits critiques comportant des éléments numériques. Le fabricant qui fait procéder à l'évaluation de conformité par un tiers peut choisir la procédure qui convient le mieux à son processus de conception et de production. Compte tenu du risque de cybersécurité encore plus grand lié à l'utilisation de produits classés comme produits critiques de classe II, l'évaluation de la conformité de ces produits devrait toujours prévoir l'intervention d'un tiers.

Amendement 29

Proposition de règlement
Considérant 46 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	(46 bis) Lorsque des produits comportant des éléments numériques sont équivalents, l'un de ces produits peut être reconnu comme représentant d'une famille ou d'une catégorie de produits aux fins de certaines procédures d'évaluation de la conformité.

Amendement 30

Proposition de règlement
Considérant 55

Texte proposé par la Commission	*Amendement*
(55) Conformément au règlement (UE) 2019/1020, les autorités de surveillance du marché sont chargées de la surveillance du marché sur le territoire de l'État membre concerné. Le présent règlement ne devrait pas empêcher les États membres de choisir les autorités compétentes pour l'accomplissement de ces tâches. Chaque État membre devrait désigner une ou plusieurs autorités de surveillance du marché sur son territoire. Les États membres peuvent choisir de désigner toute autorité existante ou nouvelle pour agir en qualité d'autorité de surveillance du marché, y compris les autorités nationales compétentes visées à l'article ***[article X]*** de la directive ***[directive XXX/XXXX*** (SRI 2)***]*** ou les autorités nationales de certification de cybersécurité désignées conformément à l'article 58 du règlement (UE) 2019/881. Les opérateurs économiques devraient coopérer pleinement avec les autorités de surveillance du marché et les autres autorités compétentes. Chaque État membre devrait communiquer à la Commission ainsi qu'aux autres États membres le nom de ses autorités de surveillance du marché et les domaines de compétence de chacune de ces autorités et veiller à ce qu'elles disposent des ressources et compétences nécessaires pour effectuer les tâches de surveillance qui leur incombent en vertu du présent règlement. Conformément à l'article 10, paragraphes 2 et 3, du règlement (UE) 2019/1020, chaque État membre devrait désigner un bureau de liaison unique chargé, entre autres, de représenter la position coordonnée des autorités de surveillance du marché et de	(55) Conformément au règlement (UE) 2019/1020, les autorités de surveillance du marché sont chargées de la surveillance du marché sur le territoire de l'État membre concerné. Le présent règlement ne devrait pas empêcher les États membres de choisir les autorités compétentes pour l'accomplissement de ces tâches. Chaque État membre devrait désigner une ou plusieurs autorités de surveillance du marché sur son territoire.Les États membres peuvent choisir de désigner toute autorité existante ou nouvelle pour agir en qualité d'autorité de surveillance du marché, y compris les autorités nationales compétentes visées à l'article ***8*** de la directive ***(UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) nº 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive*** (***UE) 2016/1148 (directive*** SRI 2) ou les autorités nationales de certification de cybersécurité désignées conformément à l'article 58 du règlement (UE) 2019/881. Les opérateurs économiques devraient coopérer pleinement avec les autorités de surveillance du marché et les autres autorités compétentes. Chaque État membre devrait communiquer à la Commission ainsi qu'aux autres États membres le nom de ses autorités de surveillance du marché et les domaines de compétence de chacune de ces autorités et veiller à ce qu'elles disposent des ressources et compétences nécessaires pour effectuer les tâches de surveillance qui leur

contribuer à la coopération entre les autorités de surveillance du marché des différents États membres.	incombent en vertu du présent règlement. Conformément à l'article 10, paragraphes 2 et 3, du règlement (UE) 2019/1020, chaque État membre devrait désigner un bureau de liaison unique chargé, entre autres, de représenter la position coordonnée des autorités de surveillance du marché et de contribuer à la coopération entre les autorités de surveillance du marché des différents États membres.

Amendement 31

Proposition de règlement
Considérant 56 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	(56 bis) Afin de permettre aux opérateurs économiques qui sont des PME et des microentreprises de faire face aux nouvelles obligations imposées par le présent règlement, la Commission devrait leur fournir des lignes directrices et des conseils faciles à comprendre, par exemple par l'intermédiaire d'un canal direct leur permettant de communiquer avec des experts lorsqu'ils ont des questions, en tenant compte de la nécessité de simplifier et de limiter les charges administratives. Lors de l'élaboration de ces lignes directrices, la Commission devrait prendre en considération les besoins des PME, afin de limiter au maximum les charges administratives et financières qui pèsent sur elles tout en facilitant leur mise en conformité avec le présent règlement. La Commission devrait consulter les parties prenantes concernées possédant une expertise dans le domaine de la cybersécurité.

Amendement 32

Proposition de règlement
Considérant 58

Texte proposé par la Commission	*Amendement*
(58) Dans certains cas, un produit comportant des éléments numériques conforme au présent règlement peut néanmoins présenter un risque de cybersécurité important ou présenter un risque pour la santé ou la sécurité des personnes, pour le respect des obligations découlant du droit de l'Union ou du droit national visant à protéger les droits fondamentaux, la disponibilité, l'authenticité, l'intégrité ou la confidentialité des services offerts au moyen d'un système d'information électronique par des entités essentielles du type visé à ***l'[annexe*** I de la directive ***XXX/XXXX*** (SRI 2)***]*** ou pour d'autres aspects de la protection de l'intérêt public. Il est donc nécessaire d'établir des règles permettant d'atténuer ces risques. En conséquence, les autorités de surveillance du marché devraient prendre des mesures pour demander à l'opérateur économique de veiller à ce que le produit ne présente plus ce risque, de le rappeler ou de le retirer, en fonction du risque. Dès qu'une autorité de surveillance du marché restreint ou interdit ainsi la libre circulation d'un produit, l'État membre devrait immédiatement informer la Commission et les autres États membres des mesures provisoires prises, en justifiant sa décision. Lorsqu'une autorité de surveillance du marché adopte de telles mesures à l'encontre de produits présentant un risque, la Commission devrait entamer sans retard des consultations avec les États membres et le ou les opérateurs économiques concernés et évaluer la mesure nationale. En fonction des résultats de cette évaluation, la Commission devrait décider si la mesure nationale est justifiée ou non. La Commission devrait adresser sa décision à tous les États membres et la communiquer immédiatement à ceux-ci	(58) Dans certains cas, un produit comportant des éléments numériques conforme au présent règlement peut néanmoins présenter un risque de cybersécurité important ou présenter un risque pour la santé ou la sécurité des personnes, pour le respect des obligations découlant du droit de l'Union ou du droit national visant à protéger les droits fondamentaux, la disponibilité, l'authenticité, l'intégrité ou la confidentialité des services offerts au moyen d'un système d'information électronique par des entités essentielles du type visé à ***l'annexe*** I de la directive ***(UE) 2022/2555*** (***directive*** SRI 2) ou pour d'autres aspects de la protection de l'intérêt public. Il est donc nécessaire d'établir des règles permettant d'atténuer ces risques. En conséquence, les autorités de surveillance du marché devraient prendre des mesures pour demander à l'opérateur économique de veiller à ce que le produit ne présente plus ce risque, de le rappeler ou de le retirer, en fonction du risque. Dès qu'une autorité de surveillance du marché restreint ou interdit ainsi la libre circulation d'un produit, l'État membre devrait immédiatement informer la Commission et les autres États membres des mesures provisoires prises, en justifiant sa décision. Lorsqu'une autorité de surveillance du marché adopte de telles mesures à l'encontre de produits présentant un risque, la Commission devrait entamer sans retard des consultations avec les États membres et le ou les opérateurs économiques concernés et évaluer la mesure nationale. En fonction des résultats de cette évaluation, la Commission devrait décider si la mesure nationale est justifiée ou non. La Commission devrait adresser sa décision à tous les États membres et la communiquer immédiatement à ceux-ci

ainsi qu'à l'opérateur ou aux opérateurs économiques concernés. Si la mesure est jugée justifiée, la Commission peut également envisager d'adopter des propositions de révision de la législation de l'Union concernée.

ainsi qu'à l'opérateur ou aux opérateurs économiques concernés. Si la mesure est jugée justifiée, la Commission peut également envisager d'adopter des propositions de révision de la législation de l'Union concernée.

Amendement 33

Proposition de règlement
Considérant 59

Texte proposé par la Commission	*Amendement*
(59) Pour les produits comportant des éléments numériques présentant un risque de cybersécurité important, et lorsqu'il y a lieu de croire que ces produits ne sont pas conformes au présent règlement, ou pour les produits qui sont conformes au présent règlement, mais présentent d'autres risques importants, tels que des risques pour la santé ou la sécurité des personnes, les droits fondamentaux ou la fourniture de services par des entités essentielles du type visé à ***l'[annexe*** I de la directive ***XXX/XXXX*** (SRI 2)***]***, la Commission peut demander à l'ENISA de procéder à une évaluation. Sur la base de cette évaluation, la Commission peut adopter, au moyen d'actes d'exécution, des mesures correctives ou restrictives au niveau de l'Union, y compris ordonner le retrait du marché ou le rappel des produits concernés, dans un délai raisonnable, proportionné à la nature du risque. La Commission ne peut recourir à une telle intervention que dans des circonstances exceptionnelles qui justifient une intervention immédiate pour préserver le bon fonctionnement du marché intérieur, et uniquement lorsqu'aucune mesure efficace n'a été prise par les autorités de surveillance pour remédier à la situation. De telles circonstances exceptionnelles peuvent être des situations d'urgence dans lesquelles, par exemple, un produit non conforme est largement mis à disposition	(59) Pour les produits comportant des éléments numériques présentant un risque de cybersécurité important, et lorsqu'il y a lieu de croire que ces produits ne sont pas conformes au présent règlement, ou pour les produits qui sont conformes au présent règlement, mais présentent d'autres risques importants, tels que des risques pour la santé ou la sécurité des personnes, les droits fondamentaux ou la fourniture de services par des entités essentielles du type visé à ***l'annexe*** I de la directive ***(UE) 2022/2555*** (***directive*** SRI 2), la Commission peut demander à l'ENISA de procéder à une évaluation. Sur la base de cette évaluation, la Commission peut adopter, au moyen d'actes d'exécution, des mesures correctives ou restrictives au niveau de l'Union, y compris ordonner le retrait du marché ou le rappel des produits concernés, dans un délai raisonnable, proportionné à la nature du risque. La Commission ne peut recourir à une telle intervention que dans des circonstances exceptionnelles qui justifient une intervention immédiate pour préserver le bon fonctionnement du marché intérieur, et uniquement lorsqu'aucune mesure efficace n'a été prise par les autorités de surveillance pour remédier à la situation. De telles circonstances exceptionnelles peuvent être des situations d'urgence dans lesquelles, par exemple, un produit non conforme est largement mis à disposition

par le fabricant dans plusieurs États membres, utilisé également dans des secteurs clés par des entités relevant du champ d'application de la ***[directive XXX/XXXX*** (SRI 2)***]***, alors qu'il contient des vulnérabilités connues qui sont exploitées par des acteurs malveillants et pour lesquelles le fabricant ne met pas de correctifs à disposition. La Commission ne peut intervenir dans de telles situations d'urgence que pour la durée des circonstances exceptionnelles et si le non-respect du présent règlement ou les risques importants présentés persistent.

par le fabricant dans plusieurs États membres, utilisé également dans des secteurs clés par des entités relevant du champ d'application de la ***directive (UE) 2022/2555*** (***directive*** SRI 2), alors qu'il contient des vulnérabilités connues qui sont exploitées par des acteurs malveillants et pour lesquelles le fabricant ne met pas de correctifs à disposition. La Commission ne peut intervenir dans de telles situations d'urgence que pour la durée des circonstances exceptionnelles et si le non-respect du présent règlement ou les risques importants présentés persistent.

Amendement 34

Proposition de règlement
Considérant 62

Texte proposé par la Commission	*Amendement*
(62) Afin de garantir que le cadre réglementaire puisse être adapté si nécessaire, il convient de déléguer à la Commission le pouvoir d'adopter des actes conformément à l'article 290 du traité en ce qui concerne les mises à jour de la liste des produits critiques figurant à l'annexe III et de préciser les définitions de ces catégories de produits. Il convient de déléguer à la Commission le pouvoir d'adopter des actes conformément audit article pour lui permettre de répertorier les produits comportant des éléments numériques couverts par d'autres règles de l'Union qui atteignent un niveau de protection identique à celui du présent règlement, en précisant si une limitation ou une exclusion du champ d'application du présent règlement serait nécessaire ainsi que la portée de cette limitation, le cas échéant. Il convient également de déléguer à la Commission le pouvoir d'adopter des actes conformément audit article en ce qui concerne la possibilité ***de rendre obligatoire la*** certification de certains	(62) Afin de garantir que le cadre réglementaire puisse être adapté si nécessaire, il convient de déléguer à la Commission le pouvoir d'adopter des actes conformément à l'article 290 du traité en ce qui concerne les mises à jour de la liste des produits critiques figurant à l'annexe III et de préciser les définitions de ces catégories de produits. Il convient de déléguer à la Commission le pouvoir d'adopter des actes conformément audit article pour lui permettre de répertorier les produits comportant des éléments numériques couverts par d'autres règles de l'Union qui atteignent un niveau de protection identique à celui du présent règlement, en précisant si une limitation ou une exclusion du champ d'application du présent règlement serait nécessaire ainsi que la portée de cette limitation, le cas échéant. Il convient également de déléguer à la Commission le pouvoir d'adopter des actes conformément audit article en ce qui concerne la possibilité ***d'instaurer une*** certification ***volontaire*** de certains produits

produits hautement critiques comportant des éléments numériques sur la base des critères de criticité énoncés dans le présent règlement, ainsi que de préciser le contenu minimal de la déclaration UE de conformité; et de compléter les éléments à inclure dans la documentation technique. 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»[33]. En particulier, afin d'assurer une participation égale à la préparation des actes délégués, le Parlement européen et le Conseil reçoivent tous les documents en même temps que les experts des États membres, et leurs experts ont systématiquement accès aux réunions des groupes d'experts de la Commission participant à la préparation des actes délégués.

[33] JO L 123 du 12.5.2016, p. 1.

hautement critiques comportant des éléments numériques sur la base des critères de criticité énoncés dans le présent règlement, ainsi que de préciser le contenu minimal de la déclaration UE de conformité; et de compléter les éléments à inclure dans la documentation technique. 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»[33]. En particulier, afin d'assurer une participation égale à la préparation des actes délégués, le Parlement européen et le Conseil reçoivent tous les documents en même temps que les experts des États membres, et leurs experts ont systématiquement accès aux réunions des groupes d'experts de la Commission participant à la préparation des actes délégués.

[33] JO L 123 du 12.5.2016, p. 1.

Amendement 35

Proposition de règlement
Considérant 63

Texte proposé par la Commission	*Amendement*
(63) Afin de garantir des conditions uniformes d'exécution du présent règlement, il convient de conférer des compétences d'exécution à la Commission, afin qu'elle puisse: spécifier le format et les éléments de la nomenclature des logiciels; préciser davantage le type d'informations, le format et la procédure des notifications relatives aux vulnérabilités activement exploitées et aux incidents soumises à l'ENISA par les fabricants; spécifier les schémas européens de certification de cybersécurité adoptés en	(63) Afin de garantir des conditions uniformes d'exécution du présent règlement, il convient de conférer des compétences d'exécution à la Commission, afin qu'elle puisse: spécifier le format et les éléments de la nomenclature des logiciels; préciser davantage le type d'informations, le format et la procédure des notifications relatives aux vulnérabilités activement exploitées et aux incidents soumises à l'ENISA par les fabricants***, sur la base des bonnes pratiques sectorielles***; spécifier les

vertu du règlement (UE) 2019/881 qui peuvent être utilisés pour démontrer la conformité aux exigences essentielles ou à des parties de celles-ci énoncées à l'annexe I du présent règlement; adopter des spécifications communes en ce qui concerne les exigences essentielles énoncées à l'annexe I; établir des spécifications techniques pour les pictogrammes ou toute autre marque liée à la sécurité des produits comportant des éléments numériques, ainsi que des mécanismes visant à promouvoir leur utilisation; décider de mesures correctives ou restrictives au niveau de l'Union dans des circonstances exceptionnelles qui justifient une intervention immédiate afin de préserver le bon fonctionnement du marché intérieur. Ces compétences devraient être exercées en conformité avec le règlement (UE) nº 182/2011 du Parlement européen et du Conseil[34].

schémas européens de certification de cybersécurité adoptés en vertu du règlement (UE) 2019/881 qui peuvent être utilisés pour démontrer la conformité aux exigences essentielles ou à des parties de celles-ci énoncées à l'annexe I du présent règlement; adopter des spécifications communes en ce qui concerne les exigences essentielles énoncées à l'annexe I; établir des spécifications techniques pour les pictogrammes ou toute autre marque liée à la sécurité des produits comportant des éléments numériques, ainsi que des mécanismes visant à promouvoir leur utilisation; décider de mesures correctives ou restrictives au niveau de l'Union dans des circonstances exceptionnelles qui justifient une intervention immédiate afin de préserver le bon fonctionnement du marché intérieur. Ces compétences devraient être exercées en conformité avec le règlement (UE) nº 182/2011 du Parlement européen et du Conseil[34].

[34] Règlement (UE) nº 182/2011 du Parlement européen et du Conseil du 16 février 2011 établissant les règles et principes généraux relatifs aux modalités de contrôle par les États membres de l'exercice des compétences d'exécution par la Commission (JO L 55 du 28.2.2011, p. 13).

[34] Règlement (UE) nº 182/2011 du Parlement européen et du Conseil du 16 février 2011 établissant les règles et principes généraux relatifs aux modalités de contrôle par les États membres de l'exercice des compétences d'exécution par la Commission (JO L 55 du 28.2.2011, p. 13).

Amendement 36

Proposition de règlement
Considérant 69

Texte proposé par la Commission	*Amendement*
(69) Il convient d'accorder un délai suffisant aux opérateurs économiques afin qu'ils s'adaptent aux exigences du présent règlement. Le présent règlement devrait s'appliquer [***24 mois] à compter de son entrée en vigueur, à l'exception des***	(69) Il convient d'accorder un délai suffisant aux opérateurs économiques afin qu'ils s'adaptent aux exigences du présent règlement. Le présent règlement devrait s'appliquer [***36*** mois] à compter de son

obligations de signalement concernant les vulnérabilités activement exploitées et les incidents, qui devraient s'appliquer [12 mois] à compter de son entrée en vigueur.	entrée en vigueur.

Amendement 37

Proposition de règlement
Article 1 – alinéa 1 – partie introductive

Texte proposé par la Commission	*Amendement*
Le présent règlement établit:	***Le présent règlement a pour objectif d'améliorer le fonctionnement du marché intérieur, tout en assurant un niveau élevé de protection des consommateurs et de cybersécurité.*** Le présent règlement établit ***des règles harmonisées concernant***:

Amendement 38

Proposition de règlement
Article 1 – alinéa 1 – point a

Texte proposé par la Commission	*Amendement*
a) ***les règles relatives à*** la mise sur le marché de produits comportant des éléments numériques afin de garantir la cybersécurité de ces produits;	a) la mise sur le marché de produits comportant des éléments numériques afin de garantir la cybersécurité de ces produits;

Amendement 39

Proposition de règlement
Article 1 – alinéa 1 – point d

Texte proposé par la Commission	*Amendement*
d) ***les règles relatives à*** la surveillance du marché et ***au*** contrôle de l'application des règles et exigences susmentionnées.	d) la surveillance du marché et ***le*** contrôle de l'application des règles et exigences susmentionnées.

Amendement 40

Proposition de règlement
Article 2 – paragraphe 1

Texte proposé par la Commission	*Amendement*
1. Le présent règlement s'applique aux produits comportant des éléments numériques dont l'utilisation prévue ou raisonnablement prévisible comprend une connexion directe ou indirecte, logique ou physique, à un dispositif ou ***à un réseau***.	1. Le présent règlement s'applique aux produits comportant des éléments numériques ***mis sur le marché*** dont l'utilisation prévue ou raisonnablement prévisible comprend une connexion directe ou indirecte, logique ou physique, à un dispositif ou ***réseau externe***.

Amendement 41

Proposition de règlement
Article 2 – paragraphe 5 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	5 bis. Le règlement ne s'applique pas aux logiciels libres et ouverts, y compris leurs codes sources et versions modifiées, sauf lorsque ces logiciels sont fournis dans le cadre d'une activité commerciale, caractérisée soit:
	i) par le prix facturé pour un produit,
	ii) par la fourniture d'une plate-forme logicielle reposant sur d'autres services monétisés par le fabricant,
	iii) par l'utilisation des données à caractère personnel générées par le logiciel pour des raisons autres qu'aux seules fins d'améliorer la sécurité, la compatibilité ou l'interopérabilité du logiciel,
	iv) par le prix facturé pour les services d'assistance technique.
	La conformité des composants libres et ouverts des produits est garantie par le fabricant du produit dans lequel ils sont intégrés.

Amendement 42

Proposition de règlement
Article 2 – paragraphe 5 ter (nouveau)

Texte proposé par la Commission	*Amendement*
	5 ter. Le présent règlement ne s'applique pas aux réseaux internes d'un produit comportant des éléments numériques si ces réseaux possèdent des points terminaux dédiés et sont complètement isolés et sécurisés par rapport à une connexion externe.

Amendement 43

Proposition de règlement
Article 2 – paragraphe 5 quater (nouveau)

Texte proposé par la Commission	*Amendement*
	5 quater. Le présent règlement ne s'applique pas aux pièces de rechange destinées exclusivement à remplacer les pièces défectueuses de produits comportant des éléments numériques en vue de restaurer leur fonctionnalité.

Amendement 44

Proposition de règlement
Article 3 – alinéa 1 – point 1

Texte proposé par la Commission	*Amendement*
1) «produit comportant des éléments numériques»: tout produit logiciel ou matériel ***et ses solutions de traitement de données à distance***, y compris les composants logiciels ou matériels ***destinées*** à être mis sur le marché séparément;	1) «produit comportant des éléments numériques»: tout produit logiciel ou matériel, y compris les composants logiciels ou matériels ***destinés*** à être mis sur le marché séparément;

Amendement 45

Proposition de règlement
Article 3 – alinéa 1 – point 2

Texte proposé par la Commission	*Amendement*
2) «traitement de données à distance»: tout traitement de données à distance pour lequel le logiciel est conçu et développé par le fabricant ou sous la responsabilité de ce dernier, et dont l'absence empêcherait le produit comportant des éléments numériques d'exécuter une de ses fonctions;	***supprimé***

Amendement 46

Proposition de règlement
Article 3– alinéa 1 – point 6 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	6 bis) «logiciel ouvert»: un logiciel distribué sous une licence qui autorise les utilisateurs à l'exécuter, à le copier, à le distribuer, à l'étudier, à le modifier et à l'améliorer librement, ainsi qu'à l'intégrer en tant que composant dans d'autres produits, à le fournir en tant que service ou à assurer une assistance commerciale connexe;

Amendement 47

Proposition de règlement
Article 3 – alinéa 1 – point 18

Texte proposé par la Commission	*Amendement*
18) «fabricant»: toute personne physique ou morale qui développe ou fabrique des produits comportant des éléments numériques ou fait concevoir, développer ou fabriquer des produits comportant des éléments numériques, et les commercialise sous son propre nom ou sa	*(Ne concerne pas la version française.)*

propre marque, à titre onéreux ou gratuit;

Amendement 48

Proposition de règlement
Article 3 – alinéa 1 – point 19

Texte proposé par la Commission	*Amendement*
19) «mandataire»: toute personne physique ou morale établie dans l'Union ayant reçu mandat écrit d'un fabricant pour agir en son nom aux fins de l'accomplissement de tâches déterminées;	19) «mandataire»: toute personne physique ou morale établie dans l'Union ayant reçu mandat écrit d'un fabricant pour agir en son nom aux fins de l'accomplissement de tâches déterminées ***qui sont liées aux obligations incombant au fabricant***;

Amendement 49

Proposition de règlement
Article 3 – alinéa 1 – point 23 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	23 bis) «rappel»: un rappel au sens de l'article 3, point 22, du règlement (UE) 2019/1020;

Amendement 50

Proposition de règlement
Article 3 – alinéa 1 – point 26

Texte proposé par la Commission	*Amendement*
26) «mauvaise utilisation raisonnablement prévisible»: l'utilisation d'un produit comportant des éléments numériques d'une manière qui n'est pas conforme à son utilisation prévue, mais qui peut résulter d'un comportement humain raisonnablement prévisible ou d'une interaction avec d'autres systèmes;	***supprimé***

Amendement 51

Proposition de règlement
Article 3 – alinéa 1 – point 31

Texte proposé par la Commission	*Amendement*
31) «modification substantielle»: une modification apportée au produit comportant des éléments numériques à la suite de sa mise sur le marché, qui a une incidence sur la conformité du produit comportant des éléments numériques aux exigences essentielles énoncées à l'annexe I, section 1, ou entraîne une modification de l'utilisation prévue pour laquelle le produit comportant des éléments numériques a été évalué;	31) «modification substantielle»: une modification apportée au produit comportant des éléments numériques***, à l'exception des mises à jour de sécurité et de maintenance,*** à la suite de sa mise sur le marché, qui a une incidence sur la conformité du produit comportant des éléments numériques aux exigences essentielles énoncées à l'annexe I, section 1, ou entraîne une modification de l'utilisation prévue pour laquelle le produit comportant des éléments numériques a été évalué;

Amendement 52

Proposition de règlement
Article 3 – alinéa 1 – point 39

Texte proposé par la Commission	*Amendement*
39) «vulnérabilité activement exploitée»: une vulnérabilité pour laquelle il existe des preuves fiables qu'un code malveillant a été exécuté par un acteur sur un système sans l'autorisation du propriétaire du système;	39) «vulnérabilité activement exploitée»: une vulnérabilité ***corrigée*** pour laquelle il existe des preuves fiables qu'un code malveillant a été exécuté par un acteur sur un système sans l'autorisation du propriétaire du système;

Amendement 53

Proposition de règlement
Article 3 – alinéa 1 – point 40 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	40 bis) «quasi-produit comportant des éléments numériques»: un objet matériel qui est incapable de fonctionner seul et qui est uniquement fabriqué dans le but

	d'être incorporé ou assemblé à un produit comportant des éléments numériques ou à un autre quasi-produit comportant des éléments numériques, et dont la conformité ne peut être évaluée de manière efficace qu'en tenant compte de la manière dont il est incorporé au produit final prévu comportant des éléments numériques;

Amendement 54

Proposition de règlement
Article 3 – alinéa 1 – point 40 ter (nouveau)

Texte proposé par la Commission	*Amendement*
	40 ter) «cycle de vie»: la période débutant au moment où un produit couvert par le présent règlement est mis sur le marché ou mis en service jusqu'au moment où il est retiré, comprenant la durée réelle pendant laquelle le produit peut être utilisé et les phases de transport, d'assemblage, de démontage, de mise hors service et de mise au rebut ou autres modifications physiques ou numériques prévues par le fabricant;

Amendement 55

Proposition de règlement
Article 4 – paragraphe 1

Texte proposé par la Commission	*Amendement*
1. Les États membres n'empêchent pas, pour les aspects relevant du présent règlement, la mise à disposition sur le marché de produits comportant des éléments numériques conformes au présent règlement.	1. Les États membres n'empêchent pas, pour les aspects relevant du présent règlement, la mise à disposition sur le marché de produits comportant des éléments numériques ***ou de quasi-produits comportant des éléments numériques*** conformes au présent règlement.

Amendement 56

Proposition de règlement
Article 4 – paragraphe 2

Texte proposé par la Commission	*Amendement*
2. Lors de foires commerciales, d'expositions, de démonstrations ou d'événements similaires, les États membres n'empêchent pas la présentation et l'utilisation d'un produit comportant des éléments numériques non conforme au présent règlement.	2. Lors de foires commerciales, d'expositions, de démonstrations ou d'événements similaires, les États membres n'empêchent pas la présentation et l'utilisation d'un produit comportant des éléments numériques***, d'un prototype de produit comportant des éléments numériques ou d'un quasi-produit comportant des éléments numériques qui n'est pas*** non ***conforme au présent règlement, pour autant que le produit comportant des éléments numériques soit utilisé exclusivement à des fins de présentation pendant l'événement et qu'une marque visible indique clairement qu'il n'est pas*** conforme au présent règlement.

Amendement 57

Proposition de règlement
Article 4 – paragraphe 3

Texte proposé par la Commission	*Amendement*
3. Les États membres n'empêchent pas la mise à disposition de ***logiciels inachevés qui ne sont*** pas ***conformes*** au présent règlement, à condition ***que le logiciel*** ne soit mis à disposition que ***pour*** une ***durée limitée nécessaire*** à des fins d'essai et qu'une marque visible indique clairement que le logiciel n'est pas conforme au présent règlement et qu'il ne sera pas disponible sur le marché à d'autres fins que les essais.	3. Les États membres n'empêchent pas la mise à disposition ***d'un produit comportant des éléments numériques inachevé ou d'un prototype*** de ***produit comportant des éléments numériques qui n'est*** pas ***conforme*** au présent règlement, à condition ***qu'il*** ne soit mis à disposition que ***dans*** une ***version non destinée à la production*** à des fins d'essai et qu'une marque visible indique clairement que le logiciel n'est pas conforme au présent règlement et qu'il ne sera pas disponible sur le marché à d'autres fins que les essais.

Amendement 58

Proposition de règlement
Article 4 – paragraphe 3 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	3 bis. Le présent règlement n'empêche pas les États membres de soumettre des produits comportant des éléments numériques à des mesures supplémentaires lorsque ces produits spécifiques seront utilisés à des fins militaires, de défense ou de sécurité nationale, conformément au droit national et au droit de l'Union, et que de telles mesures sont nécessaires et proportionnées en vue de la réalisation de ces objectifs.

Amendement 59

Proposition de règlement
Article 5 – alinéa 1 – point 1

Texte proposé par la Commission	*Amendement*
1) s'ils satisfont aux exigences essentielles énoncées à l'annexe I, section 1, à condition qu'ils soient correctement installés, entretenus, utilisés conformément à l'utilisation prévue ou dans des conditions raisonnablement prévisibles et, le cas échéant, ***mis*** à jour, et	1) s'ils satisfont aux exigences essentielles énoncées à l'annexe I, section 1, à condition qu'ils soient correctement installés, entretenus, utilisés conformément à l'utilisation prévue ou dans des conditions raisonnablement prévisibles et ***qu'ils bénéficient***, le cas échéant, ***des mises*** à jour ***de sécurité nécessaires***, et

Amendement 60

Proposition de règlement
Article 6 – paragraphe 1

Texte proposé par la Commission	*Amendement*
1. Les produits comportant des éléments numériques relevant d'une catégorie qui figure à l'annexe III sont	1. Les produits comportant des éléments numériques relevant d'une catégorie qui figure à l'annexe III sont

considérés comme des produits critiques comportant des éléments numériques. Les produits dont la fonctionnalité de base est celle d'une catégorie énumérée à l'annexe III du présent règlement sont considérés comme relevant de cette catégorie. Les catégories de produits critiques comportant des éléments numériques sont réparties entre les classes I et II, comme indiqué à l'annexe III, en fonction du niveau de risque de cybersécurité lié à ces produits.	considérés comme des produits critiques comportant des éléments numériques. ***Seuls*** les produits dont la fonctionnalité de base est celle d'une catégorie énumérée à l'annexe III du présent règlement sont considérés comme relevant de cette catégorie. Les catégories de produits critiques comportant des éléments numériques sont réparties entre les classes I et II, comme indiqué à l'annexe III, en fonction du niveau de risque de cybersécurité lié à ces produits. ***L'intégration dans un produit à faible niveau de criticité d'un composant présentant un niveau de criticité plus élevé ne modifie pas nécessairement le niveau de criticité du produit dans lequel le composant est intégré.***

Amendement 61

Proposition de règlement
Article 6 – paragraphe 2 – point b

Texte proposé par la Commission	*Amendement*
b) l'utilisation prévue dans des ***environnements sensibles, y compris dans des environnements industriels*** ou par des entités essentielles du type visé à l'annexe [annexe I] de la directive [directive XXX/XXXX (SRI 2)];	b) l'utilisation prévue dans des ***applications critiques au sein d'environnements sensibles*** ou par des entités essentielles du type visé à l'annexe [annexe I] de la directive [directive XXX/XXXX (SRI 2)];

Amendement 62

Proposition de règlement
Article 6 – paragraphe 2 – point c

Texte proposé par la Commission	*Amendement*
c) la finalité prévue de l'exécution de fonctions critiques ou sensibles, telles que le traitement de données à caractère personnel;	c) la finalité prévue ***et l'étendue*** de l'exécution de fonctions critiques ou sensibles, telles que le traitement de données à caractère personnel;

Amendement 63

Proposition de règlement
Article 6 – paragraphe 4

Texte proposé par la Commission	*Amendement*
4. Les produits critiques comportant des éléments numériques sont soumis aux procédures d'évaluation de la conformité visées à l'article 24, paragraphes 2 et 3.	4. Les produits critiques comportant des éléments numériques sont soumis aux procédures d'évaluation de la conformité visées à l'article 24, paragraphes 2 et 3. ***À titre d'exception, les micro et petites entreprises peuvent employer la procédure visée à l'article 24, paragraphe 2.***

Amendement 64

Proposition de règlement
Article 6 – paragraphe 5 – partie introductive

Texte proposé par la Commission	*Amendement*
5. La Commission est habilitée à adopter des actes délégués conformément à l'article 50 pour compléter le présent règlement en précisant les catégories de produits hautement critiques comportant des éléments numériques pour lesquels les fabricants ***sont tenus d'obtenir*** un certificat de cybersécurité européen dans le cadre d'un schéma européen de certification de cybersécurité en vertu du règlement (UE) 2019/881 afin de démontrer la conformité aux exigences essentielles énoncées à l'annexe I, ou à des parties de ces exigences. Lorsqu'elle détermine ces catégories de produits hautement critiques comportant des éléments numériques, la Commission tient compte du niveau de risque de cybersécurité lié à la catégorie de produits comportant des éléments numériques, à la lumière d'un ou de plusieurs des critères énumérés au paragraphe 2, ainsi que d'une évaluation visant à déterminer si cette catégorie de produits est:	5. La Commission est habilitée à adopter des actes délégués conformément à l'article 50 pour compléter le présent règlement en précisant les catégories de produits hautement critiques comportant des éléments numériques pour lesquels les fabricants ***peuvent obtenir*** un certificat de cybersécurité européen dans le cadre d'un schéma européen de certification de cybersécurité en vertu du règlement (UE) 2019/881 afin de démontrer la conformité aux exigences essentielles énoncées à l'annexe I, ou à des parties de ces exigences. Lorsqu'elle détermine ces catégories de produits hautement critiques comportant des éléments numériques, la Commission tient compte du niveau de risque de cybersécurité lié à la catégorie de produits comportant des éléments numériques, à la lumière d'un ou de plusieurs des critères énumérés au paragraphe 2, ainsi que d'une évaluation visant à déterminer si cette catégorie de produits est:

Amendement 65

Proposition de règlement
Article 8 – paragraphe 1

Texte proposé par la Commission	*Amendement*
1. Les produits comportant des éléments numériques classés comme systèmes d'IA à haut risque conformément à l'article [article 6] du règlement [législation sur l'IA] qui relèvent du champ d'application du présent règlement et satisfont aux exigences essentielles énoncées à l'annexe I, section 1, du présent règlement sont, lorsque les processus mis en place par le fabricant sont conformes aux exigences essentielles énoncées à l'annexe I, section 2, réputés conformes aux exigences de cybersécurité énoncées à l'article [article 15] du règlement [législation sur l'IA], sans préjudice des autres exigences en matière d'exactitude et de robustesse figurant à l'article susmentionné, et dans la mesure où le niveau de protection requis par ces exigences est démontré par la déclaration UE de conformité délivrée en vertu du présent règlement.	1. Les produits comportant des éléments numériques ***ou les quasi-produits comportant des éléments numériques*** classés comme systèmes d'IA à haut risque conformément à l'article [article 6] du règlement [législation sur l'IA] qui relèvent du champ d'application du présent règlement et satisfont aux exigences essentielles énoncées à l'annexe I, section 1, du présent règlement sont, lorsque les processus mis en place par le fabricant sont conformes aux exigences essentielles énoncées à l'annexe I, section 2, réputés conformes aux exigences de cybersécurité énoncées à l'article [article 15] du règlement [législation sur l'IA], sans préjudice des autres exigences en matière d'exactitude et de robustesse figurant à l'article susmentionné, et dans la mesure où le niveau de protection requis par ces exigences est démontré par la déclaration UE de conformité délivrée en vertu du présent règlement.

Amendement 66

Proposition de règlement
Article 8 – paragraphe 2

Texte proposé par la Commission	*Amendement*
2. Pour les produits et les exigences de cybersécurité visés au paragraphe 1, la procédure d'évaluation de la conformité pertinente prévue ***à l'article [article 43]*** du règlement [législation sur l'IA] s'applique. Aux fins de cette évaluation, les organismes notifiés qui sont habilités à contrôler la conformité des systèmes d'IA à haut risque au titre du règlement [législation sur l'IA] sont également	2. Pour les produits et les exigences de cybersécurité visés au paragraphe 1, la procédure d'évaluation de la conformité pertinente prévue ***par les [dispositions applicables]*** du règlement [législation sur l'IA] s'applique. Aux fins de cette évaluation, les organismes notifiés qui sont habilités à contrôler la conformité des systèmes d'IA à haut risque au titre du règlement [législation sur l'IA] sont

habilités à contrôler la conformité des systèmes d'IA à haut risque entrant dans le champ d'application du présent règlement aux exigences énoncées à l'annexe I du présent règlement***, à condition que la conformité de ces organismes notifiés aux exigences énoncées à l'article 29 du présent règlement ait été évaluée dans le cadre de la procédure de notification prévue par le règlement [législation sur l'IA]***.

également habilités à contrôler la conformité des systèmes d'IA à haut risque entrant dans le champ d'application du présent règlement aux exigences énoncées à l'annexe I du présent règlement.

Amendement 67

Proposition de règlement
Article 8 – paragraphe 3

Texte proposé par la Commission	*Amendement*
3. Par dérogation au paragraphe 2, les produits critiques comportant des éléments numériques énumérés à l'annexe III du présent règlement, qui doivent faire l'objet des procédures d'évaluation de la conformité prévues par l'article 24, paragraphe 2, points a) et b), et à l'article 24, paragraphe 3, points a) et b) du présent règlement, et qui sont également classés comme systèmes d'IA à haut risque conformément à l'article [article 6] du règlement [législation sur l'IA] et auxquels s'applique la procédure d'évaluation de la conformité fondée sur le contrôle interne prévue à l'annexe [VI] du règlement [législation sur l'IA], sont soumis aux procédures d'évaluation de la conformité requises par le présent règlement en ce qui concerne les exigences essentielles du présent règlement.	***supprimé***

Amendement 68

Proposition de règlement
Article 9 – alinéa 1

Texte proposé par la Commission	*Amendement*
Les machines et produits connexes relevant du champ d'application du règlement [proposition de règlement sur les machines et produits connexes] qui sont des produits comportant des éléments numériques au sens du présent règlement et pour lesquels une déclaration UE de conformité a été délivrée sur la base du présent règlement sont réputés conformes aux exigences essentielles de santé et de sécurité énoncées à l'annexe [annexe III, sections 1.1.9 et 1.2.1] du règlement [proposition de règlement sur les machines et produits connexes], en ce qui concerne la protection contre la corruption ainsi que la sécurité et la fiabilité des systèmes de commande, et dans la mesure où le niveau de protection requis par ces exigences est démontré dans la déclaration UE de conformité délivrée en vertu du présent règlement.	Les machines et produits connexes relevant du champ d'application du règlement [proposition de règlement sur les machines et produits connexes] qui sont des produits comportant des éléments numériques ***ou des quasi-produits comportant des éléments numériques*** au sens du présent règlement et pour lesquels une déclaration UE de conformité a été délivrée sur la base du présent règlement sont réputés conformes aux exigences essentielles de santé et de sécurité énoncées à l'annexe [annexe III, sections 1.1.9 et 1.2.1] du règlement [proposition de règlement sur les machines et produits connexes], en ce qui concerne la protection contre la corruption ainsi que la sécurité et la fiabilité des systèmes de commande, et dans la mesure où le niveau de protection requis par ces exigences est démontré dans la déclaration UE de conformité délivrée en vertu du présent règlement.

Amendement 69

Proposition de règlement
Article 10 – paragraphe -1 (nouveau)

Texte proposé par la Commission	*Amendement*
	-1. Les fabricants de logiciels qui sont considérés comme des microentreprises au sens de la recommandation 2003/361/CE de la Commission font tout ce qui est en leur pouvoir pour se conformer aux exigences du présent règlement dans les six mois suivant la mise sur le marché d'un logiciel. Cette disposition ne s'applique pas aux produits hautement critiques comportant des éléments numériques.

Amendement 70

Proposition de règlement
Article 10 – paragraphe 1

Texte proposé par la Commission	*Amendement*
1. Le fabricant s'assure, lorsqu'il met sur le marché un produit comportant des éléments numériques, que celui-ci a été conçu, développé et fabriqué conformément aux exigences essentielles énoncées à l'annexe I, section 1.	*(Ne concerne pas la version française.)*

Amendement 71

Proposition de règlement
Article 10 – paragraphe 4

Texte proposé par la Commission	*Amendement*
4. Aux fins du respect de l'obligation énoncée au paragraphe 1, le fabricant fait preuve de la diligence nécessaire lorsqu'il intègre dans des produits comportant des éléments numériques des composants obtenus auprès de tiers. Il ***veille*** à ce que ces composants ne compromettent pas la sécurité du produit comportant des éléments numériques.	4. Aux fins du respect de l'obligation énoncée au paragraphe 1, le fabricant fait preuve de la diligence nécessaire lorsqu'il intègre dans des produits comportant des éléments numériques des composants obtenus auprès de tiers. Il ***incombe au fabricant de veiller*** à ce que ces composants ne compromettent pas la sécurité du produit comportant des éléments numériques.

Amendement 72

Proposition de règlement
Article 10 – paragraphe 4 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	4 bis. Lorsqu'ils fournissent de tels composants au fabricant du produit fini, les fabricants des composants lui communiquent les informations et les documents nécessaires pour lui permettre de satisfaire aux exigences du présent règlement. Ces informations sont fournies gratuitement.

Amendement 73

Proposition de règlement
Article 10 – paragraphe 6 – alinéa 1

Texte proposé par la Commission	*Amendement*
Lorsqu'il met sur le marché un produit comportant des éléments numériques, et pendant la durée de vie prévue du produit ou pendant une période de cinq ans à compter de la mise sur le marché de celui-ci, la plus ***courte*** des deux durées étant retenue, le fabricant veille à ce que les vulnérabilités de ce produit soient gérées efficacement et conformément aux exigences essentielles énoncées à l'annexe I, section 2.	Lorsqu'il met sur le marché un produit comportant des éléments numériques, et pendant la durée de vie prévue du produit ***au moment de sa mise sur le marché*** ou pendant une période de cinq ans à compter de la mise sur le marché de celui-ci, la plus ***longue*** des deux durées étant retenue, le fabricant veille à ce que les vulnérabilités de ce produit soient gérées efficacement et conformément aux exigences essentielles énoncées à l'annexe I, section 2***, à condition que le fabricant en ait la maîtrise***.

Amendement 74

Proposition de règlement
Article 10 – paragraphe 7 – alinéa 3 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	Lorsqu'une mise à jour du logiciel est effectuée, le fabricant n'est pas tenu de procéder à une autre évaluation de la conformité du produit comportant des éléments numériques, sauf si la mise à jour logicielle entraîne une modification substantielle du produit comportant des éléments numériques au sens de l'article 3, paragraphe 31, du présent règlement.

Amendement 75

Proposition de règlement
Article 10 – paragraphe 9

Texte proposé par la Commission	*Amendement*
9. Le fabricant veille à ce que des procédures soient en place pour que la conformité des produits comportant des éléments numériques produits en série reste assurée. Le fabricant tient dûment compte des modifications du processus de développement et de production ou de la conception ou des caractéristiques du produit comportant des éléments numériques, ainsi que des modifications des normes harmonisées, des schémas européens de certification de cybersécurité ou des spécifications techniques visées à l'article 19 au regard desquelles la conformité du produit comportant des éléments numériques est déclarée ou en application desquelles sa conformité est vérifiée.	9. Le fabricant veille à ce que des procédures soient en place pour que la conformité des produits comportant des éléments numériques produits en série reste assurée. Le fabricant tient dûment compte des modifications du processus de développement et de production ou de la conception ou des caractéristiques du produit comportant des éléments numériques, ainsi que des modifications des normes harmonisées, des schémas européens de certification de cybersécurité ou des spécifications techniques visées à l'article 19 au regard desquelles la conformité du produit comportant des éléments numériques est déclarée ou en application desquelles sa conformité est vérifiée. ***Au fur et à mesure de l'apparition de nouvelles connaissances, techniques ou normes, qui n'étaient pas disponibles au moment de la conception d'un produit de série, le fabricant peut envisager de mettre en œuvre ces améliorations périodiquement pour les nouvelles générations de produits.***

Amendement 76

Proposition de règlement
Article 10 – paragraphe 9 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	9 bis. Les fabricants font connaître publiquement la durée de vie prévue de leurs produits de manière claire et compréhensible.

Amendement 77

Proposition de règlement
Article 10 – paragraphe 12

Texte proposé par la Commission	*Amendement*
12. Dès la mise sur le marché et pendant la durée de vie prévue d'un produit comportant des éléments numériques ou pendant une période de cinq ans après sa mise sur le marché, la durée la plus ***courte*** étant retenue, le fabricant qui considère ou a des raisons de croire que le produit comportant des éléments numériques ou les processus mis en place par le fabricant ne sont pas conformes aux exigences essentielles énoncées à l'annexe I prend immédiatement les mesures correctives nécessaires pour mettre ce produit comportant des éléments numériques ou les processus du fabricant en conformité, ou pour procéder à leur retrait ou à leur rappel, selon le cas.	12. Dès la mise sur le marché et pendant la durée de vie prévue d'un produit comportant des éléments numériques ou pendant une période de cinq ans après sa mise sur le marché, la durée la plus ***longue*** étant retenue, le fabricant qui considère ou a des raisons de croire que le produit comportant des éléments numériques ou les processus mis en place par le fabricant ne sont pas conformes aux exigences essentielles énoncées à l'annexe I prend immédiatement les mesures correctives nécessaires pour mettre ce produit comportant des éléments numériques ou les processus du fabricant en conformité, ou pour procéder à leur retrait ou à leur rappel, selon le cas.

Amendement 78

Proposition de règlement
Article 11 – paragraphe 1

Texte proposé par la Commission	*Amendement*
1. Le fabricant notifie à l'ENISA, dans les meilleurs délais et, en tout état de cause, au plus tard ***24 heures*** après en avoir eu connaissance, toute vulnérabilité activement exploitée contenue dans le produit comportant des éléments numériques. ***La notification contient des précisions concernant cette vulnérabilité et, le cas échéant, toute mesure prise pour y remédier ou en atténuer les effets. Dès réception de cette notification, l'ENISA la transmet, sans retard indu, sauf pour des motifs justifiés ayant trait au risque de cybersécurité, au CSIRT désigné aux fins de la divulgation coordonnée des vulnérabilités conformément à l'article [X] de la directive [XXX/XXXX (SRI2)] des États membres concernés et informe l'autorité de surveillance du marché de la vulnérabilité***	1. Le fabricant notifie à l'ENISA, dans les meilleurs délais et, en tout état de cause, ***48 heures*** au plus tard après en avoir eu connaissance, ***au moyen d'une alerte précoce,*** toute vulnérabilité activement exploitée contenue dans le produit comportant des éléments numériques.

notifiée.

Amendement 79

Proposition de règlement
Article 11 – paragraphe 1 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	1 bis. Les fabricants, dans les meilleurs délais après avoir eu connaissance de vulnérabilités activement exploitées ayant une incidence importante sur la sécurité du produit comportant des éléments numériques, communiquent à l'ENISA des précisions supplémentaires sur ladite vulnérabilité exploitée.

Amendement 80

Proposition de règlement
Article 11 – paragraphe 1 ter (nouveau)

Texte proposé par la Commission	*Amendement*
	1 ter. Toute autre vulnérabilité n'ayant pas d'incidence importante sur la sécurité du produit comportant des éléments numériques est signalée à l'ENISA une fois traitée.

Amendement 81

Proposition de règlement
Article 11 – paragraphe 1 quater (nouveau)

Texte proposé par la Commission	*Amendement*
	1 quater. La notification contient des précisions concernant cette vulnérabilité et, le cas échéant, toute mesure prise pour y remédier ou en atténuer les effets, ainsi que toute mesure recommandée d'atténuation des risques. Dès réception de cette notification, l'ENISA la transmet,

sans retard indu, sauf pour des motifs justifiés ayant trait au risque de cybersécurité, au CSIRT désigné aux fins de la divulgation coordonnée des vulnérabilités conformément à l'article [X] de la directive [XXX/XXXX (SRI2)] des États membres concernés et informe immédiatement l'autorité de surveillance du marché de l'existence d'une vulnérabilité et, le cas échéant, des mesures d'atténuation des risques potentiels. En l'absence de mesure corrective ou d'atténuation pour une vulnérabilité notifiée, l'ENISA veille à ce que les informations concernant cette vulnérabilité soient partagées conformément à des protocoles de sécurité stricts et selon le principe du besoin d'en connaître.

Amendement 82

Proposition de règlement
Article 11 – paragraphe 2

Texte proposé par la Commission	*Amendement*
2. Le fabricant notifie à l'ENISA, dans les meilleurs délais et, en tout état de cause, au plus tard 24 heures après en avoir eu connaissance, tout incident ayant ***un impact*** sur la sécurité du produit comportant des éléments numériques. L'ENISA transmet sans retard indu, sauf pour des motifs justifiés ayant trait au risque de cybersécurité, les notifications au point de contact unique désigné conformément à l'article [article X] de la directive [XXX/XXXX (SRI 2)] des États membres concernés et informe l'autorité de surveillance du marché des incidents notifiés. La notification d'incident comprend ***des*** informations sur la gravité et l'impact de l'incident et, le cas échéant, indique si le fabricant soupçonne des actes illicites ou malveillants d'être à l'origine de l'incident ou s'il considère que ce	2. Le fabricant notifie à l'ENISA, dans les meilleurs délais et, en tout état de cause, au plus tard 24 heures après en avoir eu connaissance***, au moyen d'une alerte précoce***, tout incident ayant ***des répercussions importantes*** sur la sécurité du produit comportant des éléments numériques. ***En outre, le fabricant communique à l'ENISA, dans les meilleurs délais et en tout état de cause dans les 72 heures après avoir eu connaissance de l'incident important relatif au produit comportant des éléments numériques, des précisions supplémentaires sur ledit incident important.*** L'ENISA transmet sans retard indu, sauf pour des motifs justifiés ayant trait au risque de cybersécurité, les notifications au point de contact unique désigné conformément à l'article [article X] de la directive [XXX/XXXX

dernier a des répercussions transfrontières.	(SRI 2)] des États membres concernés et informe ***immédiatement*** l'autorité de surveillance du marché des incidents ***importants*** notifiés. La notification d'incident comprend ***les*** informations ***strictement nécessaires pour informer l'autorité compétente de l'incident et, lorsque cela est pertinent et proportionné au risque,*** sur la gravité et l'impact de l'incident et, le cas échéant, indique si le fabricant soupçonne des actes illicites ou malveillants d'être à l'origine de l'incident ou s'il considère que ce dernier a des répercussions transfrontières. ***Le simple fait de notifier un incident n'accroît pas la responsabilité de l'entité qui est à l'origine de la notification.***

Amendement 83

Proposition de règlement
Article 11 – paragraphe 2 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	2 bis. Les opérateurs économiques qui sont également identifiés comme des entités essentielles ou des entités importantes au titre de la SRI 2 et qui soumettent leur notification d'incident conformément à la directive SRI 2 sont réputés en conformité avec les exigences visées au point 2 du présent article.

Amendement 84

Proposition de règlement
Article 11 – paragraphe 3

Texte proposé par la Commission	*Amendement*
3. L'ENISA soumet au réseau européen d'organisations de liaison en cas de crises de cybersécurité (UE - CyCLONe) institué par l'article [l'article X] de la directive [la	3. L'ENISA soumet au réseau européen d'organisations de liaison en cas de crises de cybersécurité (UE - CyCLONe) institué par l'article [l'article X] de la directive [la directive

directive XXX/XXXX (SRI2)] les informations notifiées conformément aux paragraphes 1 et 2 si elles sont pertinentes pour la gestion coordonnée au niveau opérationnel des incidents et crises de cybersécurité ***majeurs***.	XXX/XXXX (SRI2)] les informations notifiées conformément aux paragraphes 1 et 2 si elles sont pertinentes pour la gestion coordonnée au niveau opérationnel des incidents ***importants*** et crises de cybersécurité ***d'ampleur majeure***.

Amendement 85

Proposition de règlement
Article 11 – paragraphe 4

Texte proposé par la Commission	*Amendement*
4. Dans les meilleurs délais après avoir pris connaissance ***de l'incident***, le fabricant informe les utilisateurs du produit comportant des éléments numériques de ***cet incident*** et, le cas échéant, des ***mesures correctives*** que l'utilisateur peut mettre en place pour ***en*** atténuer l'impact.	4. Dans les meilleurs délais après ***en*** avoir pris connaissance, le fabricant informe les utilisateurs du produit comportant des éléments numériques de ***l'incident important, s'il y a lieu et si celui-ci risque de leur nuire,*** et, le cas échéant, ***de toute mesure d'atténuation*** des ***risques ou mesure corrective*** que l'utilisateur peut mettre en place pour atténuer l'impact ***de l'incident important quant aux données pouvant être touchées et aux dommages éventuels***.

Amendement 86

Proposition de règlement
Article 11 – paragraphe 4 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	4 bis. Les obligations prévues aux paragraphes 1, 2 et 4 s'appliquent pendant la durée de vie du produit. Pendant la période de durée de vie prévue du produit, le fabricant fournit gratuitement des mises à jour de sécurité qui s'appliquent uniquement aux produits comportant des éléments numériques pour lesquels le fabricant a établi une déclaration UE de conformité, conformément à l'article 20 du présent règlement.

Amendement 87

Proposition de règlement
Article 11 – paragraphe 5

Texte proposé par la Commission	*Amendement*
5. La Commission peut, au moyen d'actes d'exécution, préciser plus en détail le type d'informations, le format et la procédure des notifications présentées en vertu des paragraphes 1 et 2. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 51, paragraphe 2.	5. La Commission peut, ***après avoir consulté les parties intéressées et les CSIRT,*** au moyen d'actes d'exécution, préciser plus en détail le type d'informations, le format et la procédure des notifications présentées en vertu des paragraphes 1 et 2. Ces actes d'exécution ***tiennent compte des normes européennes et internationales et*** sont adoptés en conformité avec la procédure d'examen visée à l'article 51, paragraphe 2.

Amendement 88

Proposition de règlement
Article 11 – paragraphe 6

Texte proposé par la Commission	*Amendement*
6. Sur la base des notifications reçues conformément aux paragraphes 1 et 2, l'ENISA élabore un rapport technique bisannuel sur les tendances émergentes en ce qui concerne les risques de cybersécurité dans les produits comportant des éléments numériques et le soumet au groupe de coopération visé à l'article ***[article X]*** de la directive ***[directive XXX/XXXX (SRI 2)]***. Le premier rapport de ce type est présenté dans les 24 mois suivant le début de l'application des obligations prévues aux paragraphes 1 et 2.	6. Sur la base des notifications reçues conformément aux paragraphes 1 et 2, l'ENISA élabore un rapport technique bisannuel sur les tendances émergentes en ce qui concerne les risques de cybersécurité dans les produits comportant des éléments numériques et le soumet au groupe de coopération visé à l'article ***14*** de la directive (***UE***) ***2022/2555***. Le premier rapport de ce type est présenté dans les 24 mois suivant le début de l'application des obligations prévues aux paragraphes 1 et 2.

Amendement 89

Proposition de règlement
Article 11 – paragraphe 7

Texte proposé par la Commission	*Amendement*
7. Lorsqu'il identifie une vulnérabilité dans un composant, y compris un composant open source, qui est intégré au produit comportant des éléments numériques, le fabricant signale la vulnérabilité à la personne ou à l'entité qui assure la maintenance du composant.	7. Lorsqu'il identifie une vulnérabilité dans un composant, y compris un composant open source, qui est intégré au produit comportant des éléments numériques, le fabricant signale la vulnérabilité et la mesure corrective ou d'atténuation prise à la personne ou à l'entité qui assure la maintenance du composant. ***Cela ne libère pas le fabricant de l'obligation de maintenir la conformité du produit au regard des exigences du présent règlement et ne crée aucune obligation pour les développeurs de composants libres et ouverts qui n'ont pas de relation contractuelle avec ledit fabricant.***

Amendement 90

Proposition de règlement
Article 12 – paragraphe 3 – partie introductive

Texte proposé par la Commission	*Amendement*
3. Le mandataire exécute les tâches spécifiées dans le mandat qu'il reçoit du fabricant. Le mandat autorise au minimum le mandataire:	3. Le mandataire exécute les tâches spécifiées dans le mandat qu'il reçoit du fabricant. ***Il fournit une copie du mandat aux autorités de surveillance du marché qui en font la demande.*** Le mandat autorise au minimum le mandataire:

Amendement 91

Proposition de règlement
Article 12 – paragraphe 3 – point a bis (nouveau)

Texte proposé par la Commission	*Amendement*
	a bis) lorsqu'il a une raison de croire que le produit comportant des éléments numériques en question présente un

	risque de cybersécurité, à informer le fabricant;

Amendement 92

Proposition de règlement
Article 12 – paragraphe 3 – point b

Texte proposé par la Commission	*Amendement*
b) sur requête motivée d'une autorité de surveillance du marché, à communiquer à cette dernière toutes les informations et tous les documents nécessaires pour démontrer la conformité du produit comportant des éléments numériques;	b) sur requête motivée d'une autorité de surveillance du marché, à communiquer à cette dernière toutes les informations et tous les documents nécessaires pour démontrer la ***sécurité et la*** conformité du produit comportant des éléments numériques***, dans une langue pouvant être comprise facilement par cette autorité***;

Amendement 93

Proposition de règlement
Article 12 – paragraphe 3 – point c

Texte proposé par la Commission	*Amendement*
c) à coopérer avec les autorités de surveillance du marché, à leur demande, concernant toute mesure adoptée pour éliminer les risques présentés par un produit comportant des éléments numériques relevant du mandat confié au mandataire.	c) à coopérer avec les autorités de surveillance du marché, à leur demande, concernant toute mesure adoptée pour éliminer ***efficacement*** les risques présentés par un produit comportant des éléments numériques relevant du mandat confié au mandataire.

Amendement 94

Proposition de règlement
Article 13 – paragraphe 2 – point c bis (nouveau)

Texte proposé par la Commission	*Amendement*
	c bis) tous les documents qui prouvent le respect des exigences prévues par le présent article aient été reçus par le fabricant et puissent être communiqués

pour inspection pendant une durée de dix ans.

Amendement 95

Proposition de règlement
Article 13 – paragraphe 3

Texte proposé par la Commission	*Amendement*
3. Lorsqu'un importateur considère ou a des raisons de croire qu'un produit comportant des éléments numériques ou les processus mis en place par le fabricant ne sont pas conformes aux exigences essentielles énoncées à l'annexe I, il ne met pas le produit sur le marché tant que ce produit ou les processus mis en place par le fabricant n'ont pas été mis en conformité avec les exigences essentielles énoncées à l'annexe I. En outre, lorsque le produit comportant des éléments numériques présente un risque de cybersécurité important, l'importateur en informe le fabricant et les autorités de surveillance du marché.	3. Lorsqu'un importateur considère ou a des raisons de croire***, sur la base des informations à sa disposition,*** qu'un produit comportant des éléments numériques ou les processus mis en place par le fabricant ne sont pas conformes aux exigences essentielles énoncées à l'annexe I, il ne met pas le produit sur le marché tant que ce produit ou les processus mis en place par le fabricant n'ont pas été mis en conformité avec les exigences essentielles énoncées à l'annexe I. En outre, lorsque le produit comportant des éléments numériques présente un risque de cybersécurité important, l'importateur en informe le fabricant et les autorités de surveillance du marché.

Amendement 96

Proposition de règlement
Article 13 – paragraphe 4

Texte proposé par la Commission	*Amendement*
4. L'importateur indique son nom, sa raison sociale ou sa marque déposée et les adresses postale et électronique auxquelles il peut être contacté sur le produit comportant des éléments numériques ou, lorsque cela n'est pas possible, sur l'emballage ou dans un document accompagnant le produit comportant des éléments numériques. Les coordonnées sont indiquées dans une langue aisément compréhensible par les utilisateurs et les	*(Ne concerne pas la version française.)*

autorités de surveillance du marché.

Amendement 97

Proposition de règlement
Article 13 – paragraphe 6 – alinéa 1

Texte proposé par la Commission	*Amendement*
Tout importateur qui considère ou a des raisons de croire qu'un produit comportant des éléments numériques, qu'il a mis sur le marché, ou bien les processus mis en place par son fabricant, ne sont pas conformes aux exigences essentielles énoncées à l'annexe I prend immédiatement les mesures correctives nécessaires pour mettre ce produit comportant des éléments numériques ou les processus mis en place par son fabricant en conformité avec les exigences essentielles énoncées à l'annexe I, ou pour procéder au retrait ou au rappel du produit, si nécessaire.	Tout importateur qui considère ou a des raisons de croire qu'un produit comportant des éléments numériques, qu'il a mis sur le marché, ou bien les processus mis en place par son fabricant, ne sont pas conformes aux exigences essentielles énoncées à l'annexe I prend immédiatement les mesures correctives nécessaires pour mettre ce produit comportant des éléments numériques ou les processus mis en place par son fabricant en conformité avec les exigences essentielles énoncées à l'annexe I, ou pour procéder au retrait ou au rappel du produit, si nécessaire. ***Sur la base d'une évaluation des risques, les distributeurs et les utilisateurs finals sont informés en temps utile de la non-conformité et des mesures d'atténuation des risques qu'ils peuvent prendre.***

Amendement 98

Proposition de règlement
Article 14 – paragraphe 2 – point b bis (nouveau)

Texte proposé par la Commission	*Amendement*
	b bis) il a reçu, de la part du fabricant et de l'importateur, toutes les informations et tous les documents requis par le présent règlement.

Amendement 99

Proposition de règlement
Article 16 – alinéa 1

Texte proposé par la Commission	*Amendement*
Une personne physique ou morale, autre que le fabricant, l'importateur ou le distributeur, qui apporte une modification substantielle à un produit comportant des éléments numériques est considérée comme un fabricant aux fins du présent règlement.	Une personne physique ou morale, autre que le fabricant, l'importateur ou le distributeur, qui***, dans le cadre d'une activité professionnelle,*** apporte une modification substantielle à un produit comportant des éléments numériques ***et qui met le produit à disposition sur le marché*** est considérée comme un fabricant aux fins du présent règlement.

Amendement 100

Proposition de règlement
Article 18 – paragraphe 1 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	1 bis. Conformément à l'article 10, paragraphe 1, du règlement (UE) 1025/2012, la Commission demande à une ou plusieurs organisations européennes de normalisation d'élaborer des normes harmonisées relatives aux exigences énoncées à l'annexe I.

Amendement 101

Proposition de règlement
Article 18 – paragraphe 4 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	4 bis. Conformément à l'article 10, paragraphe 1, du règlement 1025/2012, lors de l'élaboration de la demande de normalisation de produits relevant du champ d'application du présent règlement, la Commission vise une harmonisation maximale avec les normes internationales en vigueur ou dont l'application est imminente en matière de cybersécurité. Au cours des trois années

	qui suivent la date d'application du présent règlement, la Commission est habilitée à déclarer qu'une norme internationale existante respecte les exigences du présent règlement, sans aucune modification européenne, pour autant que l'observation de cette norme améliore suffisamment la sécurité des produits comportant des éléments numériques, et pour autant que la norme soit publiée dans une version séparée par l'une des organisations européennes de normalisation.

Amendement 102

Proposition de règlement
Article 19 – alinéa 1

Texte proposé par la Commission	*Amendement*
Lorsque les normes harmonisées visées à l'article 18 n'existent pas ou lorsque la Commission ***estime que les normes harmonisées pertinentes sont insuffisantes pour satisfaire aux*** exigences ***du présent règlement ou pour répondre à la demande de normalisation de la Commission, ou lorsque la procédure de normalisation rencontre des retards excessifs ou lorsqu'aucune organisation européenne*** de ***normalisation n'a accepté la demande*** de ***normes harmonisées*** de ***la Commission, la Commission est habilitée, au moyen d'actes d'exécution,*** à ***adopter des spécifications communes*** en ce qui concerne les ***exigences essentielles énoncées à l'annexe I***. Ces actes d'exécution sont adoptés ***en conformité avec la procédure d'examen visée à l'article 51, paragraphe 2.***	***1.*** La Commission ***peut adopter des actes d'exécution qui établissent des spécifications communes couvrant les*** exigences ***techniques qui offrent un moyen*** de ***se conformer aux exigences essentielles*** de ***santé et*** de ***sécurité énoncées*** à ***l'annexe I*** en ce qui concerne les ***produits relevant du champ d'application du présent règlement***. Ces actes d'exécution ***ne*** sont adoptés ***que lorsque les conditions suivantes sont remplies:***
	a) la Commission, conformément à l'article 10, paragraphe 1, du règlement (UE) nº 1025/2012, a demandé à une ou plusieurs organisations européennes de normalisation d'élaborer

une norme harmonisée relative aux exigences essentielles énoncées à l'annexe I et:

i) la demande n'a pas été acceptée; ou

ii) les normes harmonisées correspondant à cette demande ne sont pas présentées dans le délai fixé conformément à l'article 10, paragraphe 1, du règlement (UE) 1025/2012; ou

iii) les normes harmonisées ne sont pas conformes à la demande; et

b) aucune référence à des normes harmonisées couvrant les exigences énoncées à l'annexe I n'a été publiée au Journal officiel de l'Union européenne conformément au règlement (UE) nº1025/2012 et il n'est pas prévu que la publication d'une telle référence intervienne dans un délai raisonnable.

Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 48, paragraphe 3.

Amendement 103

Proposition de règlement
Article 19 – paragraphe 1 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	1 bis. Avant d'élaborer le projet d'acte d'exécution visé au paragraphe 3, la Commission informe le comité visé à l'article 22 du règlement (UE) nº 1025/2012 qu'elle considère que les conditions énoncées au paragraphe 3 sont remplies.

Amendement 104

Proposition de règlement
Article 19 – paragraphe 1 ter (nouveau)

Texte proposé par la Commission	*Amendement*
	1 ter. Lorsqu'elle élabore le projet d'acte d'exécution visé au paragraphe 1, la Commission tient compte de l'avis des organismes compétents ou du groupe d'experts et consulte dûment toutes les parties prenantes concernées.

Amendement 105

Proposition de règlement
Article 19 – paragraphe 1 quater (nouveau)

Texte proposé par la Commission	*Amendement*
	1 quater. Lorsqu'une norme harmonisée est adoptée par une organisation européenne de normalisation et proposée à la Commission en vue de la publication de sa référence au Journal officiel de l'Union européenne, la Commission évalue la norme harmonisée conformément au règlement (UE) nº 1025/2012. Lorsque la référence d'une norme harmonisée est publiée au Journal officiel de l'Union européenne, la Commission abroge les actes d'exécution visés au paragraphe 1 ou les parties de ces actes qui couvrent les mêmes exigences que celles couvertes par cette norme harmonisée.

Amendement 106

Proposition de règlement
Article 19 – paragraphe 1 quinquies (nouveau)

Texte proposé par la Commission	*Amendement*
	1 quinquies. Lorsqu'un État membre estime qu'une spécification commune ne satisfait pas entièrement aux exigences énoncées à l'annexe I, il en informe la

	Commission en lui fournissant une explication détaillée. La Commission examine cette explication détaillée et peut, s'il y a lieu, modifier l'acte d'exécution établissant la spécification commune en question.

Amendement 107

Proposition de règlement
Article 20 – paragraphe 2

Texte proposé par la Commission	*Amendement*
2. La déclaration UE de conformité est établie selon le modèle figurant à l'annexe IV et contient les éléments précisés dans les procédures d'évaluation de la conformité applicables prévues à l'annexe VI. Cette déclaration est ***constamment*** mise à jour. Elle est disponible dans ***la ou les langues requises*** par l'État membre dans lequel le produit comportant des éléments numériques est mis sur le marché ou mis à disposition.	2. La déclaration UE de conformité est établie selon le modèle figurant à l'annexe IV et contient les éléments précisés dans les procédures d'évaluation de la conformité applicables prévues à l'annexe VI. Cette déclaration est mise à jour ***selon que de besoin***. Elle est disponible dans ***une langue qui peut être facilement comprise*** par ***les autorités de*** l'État membre dans lequel le produit comportant des éléments numériques est mis sur le marché ou mis à disposition.

Amendement 108

Proposition de règlement
Article 20 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	Article 20 bis
	Déclaration UE d'incorporation pour les quasi-produits comportant des éléments numériques
	1. La déclaration UE d'incorporation est établie par le fabricant conformément à l'article 10, paragraphe 7, et atteste que le respect des exigences essentielles pertinentes énoncées à l'annexe I a été démontré.
	2. La déclaration UE d'incorporation

est établie selon le modèle figurant à l'annexe IV bis (nouvelle). Cette déclaration est mise à jour selon que de besoin. Elle est disponible dans la ou les langues requises par l'État membre dans lequel le quasi-produit comportant des éléments numériques est mis sur le marché ou mis à disposition.

3. Lorsqu'un quasi-produit comportant des éléments numériques relève de plusieurs actes de l'Union imposant une déclaration UE d'incorporation, une seule déclaration UE d'incorporation est établie pour l'ensemble de ces actes. Cette déclaration mentionne les titres des actes de l'Union concernés, ainsi que les références de leur publication.

4. La Commission est habilitée à adopter des actes délégués conformément à l'article 50 pour compléter le présent règlement aux fins d'ajouter des éléments au contenu minimal de la déclaration UE d'incorporation prévu à l'annexe IV bis (nouvelle) afin de tenir compte des progrès techniques.

Amendement 109

Proposition de règlement
Article 22 – paragraphe 1

Texte proposé par la Commission	*Amendement*
1. Le marquage CE est apposé de manière visible, lisible et indélébile sur le produit comportant des éléments numériques. Lorsque la nature du produit comportant des éléments numériques ne le permet pas ou ne le justifie pas, il est apposé sur son emballage et sur la déclaration UE de conformité mentionnée à l'article 20 qui accompagne le produit comportant des éléments numériques. Pour les produits comportant des éléments numériques qui se présentent sous la forme d'un logiciel, le marquage CE est apposé	1. Le marquage CE est apposé de manière visible, lisible et indélébile sur le produit comportant des éléments numériques. Lorsque la nature du produit comportant des éléments numériques ne le permet pas ou ne le justifie pas, il est apposé sur son emballage et sur la déclaration UE de conformité mentionnée à l'article 20 qui accompagne le produit comportant des éléments numériques. Pour les produits comportant des éléments numériques qui se présentent sous la forme d'un logiciel, le marquage CE est apposé

soit sur la déclaration UE de conformité mentionnée à l'article 20, soit sur le site web qui accompagne le logiciel.	soit sur la déclaration UE de conformité mentionnée à l'article 20, soit sur le site web qui accompagne le logiciel. ***Dans ce dernier cas, la section correspondante du site web est aisément et directement accessible aux consommateurs.***

Amendement 110

Proposition de règlement
Article 22 – paragraphe 3

Texte proposé par la Commission	*Amendement*
3. Le marquage CE est apposé avant que le produit comportant des éléments numériques ne soit mis sur le marché. Il peut être suivi d'un pictogramme ou de tout autre marquage indiquant un risque ou un usage particulier énoncés dans les actes d'exécution visés au paragraphe 6.	3. Le marquage CE est apposé avant que le produit comportant des éléments numériques ne soit mis sur le marché. Il peut être suivi d'un pictogramme ou de tout autre marquage indiquant ***aux consommateurs*** un risque ou un usage particulier énoncés dans les actes d'exécution visés au paragraphe 6.

Amendement 111

Proposition de règlement
Article 22 – paragraphe 5

Texte proposé par la Commission	*Amendement*
5. Les États membres s'appuient sur les mécanismes existants pour assurer la bonne application du régime régissant le marquage CE et prennent les mesures nécessaires en cas d'usage abusif de ce marquage. Lorsque le produit comportant des éléments numériques relève d'autres actes législatifs de l'Union qui prévoient aussi l'apposition du marquage CE, le marquage CE indique que le produit satisfait également aux exigences de ces autres actes législatifs.	5. Les États membres s'appuient sur les mécanismes existants pour assurer la bonne application ***harmonisée*** du régime régissant le marquage CE et prennent les mesures nécessaires ***de façon coordonnée*** en cas d'usage abusif de ce marquage. Lorsque le produit comportant des éléments numériques relève d'autres actes législatifs de l'Union qui prévoient aussi l'apposition du marquage CE, le marquage CE indique que le produit satisfait également aux exigences de ces autres actes législatifs.

Amendement 112

Proposition de règlement
Article 22 – paragraphe 6

Texte proposé par la Commission	*Amendement*
6. La Commission peut, au moyen d'actes ***d'exécution***, définir des spécifications techniques pour les pictogrammes ou tout autre marquage en lien avec la sécurité du produit comportant des éléments numériques, ainsi que des mécanismes visant à promouvoir leur utilisation. Ces actes ***d'exécution*** sont adoptés en conformité avec la procédure ***d'examen*** visée à l'article ***51, paragraphe 2***.	6. La Commission peut, au moyen d'actes ***délégués***, définir des spécifications techniques pour ***les systèmes d'étiquetage, y compris les étiquettes harmonisées,*** les pictogrammes ou tout autre marquage en lien avec la sécurité du produit comportant des éléments numériques, ainsi que des mécanismes visant à promouvoir leur utilisation ***chez les entreprises et les consommateurs et à sensibiliser le public à la sécurité des produits comportant des éléments numériques***. Ces actes ***délégués*** sont adoptés en conformité avec la procédure visée à l'article ***50***.

Amendement 113

Proposition de règlement
Article 22 – paragraphe 6 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	6 bis. Un quasi-produit comportant des éléments numériques ne porte pas le marquage CE prévu au titre du présent règlement, sans préjudice des dispositions de marquage qui résultent de tout autre acte législatif de l'Union applicable.

Amendement 114

Proposition de règlement
Article 22 – paragraphe 6 ter (nouveau)

Texte proposé par la Commission	*Amendement*
	6 ter. La Commission adopte des lignes directrices et fournit des conseils aux opérateurs économiques, en particulier à ceux qui sont considérés comme

	des PME, y compris les microentreprises, sur la mise en œuvre du présent règlement. Ces lignes directrices et ces conseils visent en particulier à simplifier et à limiter la charge administrative et financière, tout en garantissant une application efficace et cohérente du présent règlement conformément à l'objectif général consistant à garantir la sécurité des produits et la protection des consommateurs. La Commission devrait consulter les parties prenantes concernées possédant une expertise dans le domaine de la cybersécurité.

Amendement 115

Proposition de règlement
Article 23 – paragraphe 2

Texte proposé par la Commission	*Amendement*
2. La documentation technique est établie avant que le produit comportant des éléments numériques ne soit mis sur le marché et fait l'objet de mises à jour régulières, le cas échéant, pendant la durée de vie prévue du produit ou pendant une période de cinq ans après la mise sur le marché d'un produit comportant des éléments numériques, la durée la plus ***courte*** étant retenue.	2. La documentation technique est établie avant que le produit comportant des éléments numériques ne soit mis sur le marché et fait l'objet de mises à jour régulières, le cas échéant, pendant la durée de vie prévue du produit ou pendant une période de cinq ans après la mise sur le marché d'un produit comportant des éléments numériques, la durée la plus ***longue*** étant retenue.

Amendement 116

Proposition de règlement
Article 23 – paragraphe 3

Texte proposé par la Commission	*Amendement*
3. Pour les produits comportant des éléments numériques ***mentionnés à l'article 8 et à l'article 24, paragraphe 4,*** qui relèvent aussi d'autres actes législatifs de l'Union, une seule documentation technique est établie, contenant les	3. Pour les produits comportant des éléments numériques qui relèvent aussi d'autres actes législatifs de l'Union, une seule documentation technique est établie, contenant les informations visées à l'annexe V du présent règlement ainsi que

informations visées à l'annexe V du présent règlement ainsi que les informations requises en vertu de ces actes de l'Union.	les informations requises en vertu de ces actes de l'Union.

Amendement 117

Proposition de règlement
Article 23 – paragraphe 5

Texte proposé par la Commission	*Amendement*
5. La Commission est habilitée à adopter des actes délégués conformément à l'article 50 pour compléter le présent règlement aux fins d'inclure les éléments requis dans la documentation technique figurant à l'annexe V pour tenir compte des progrès techniques ainsi que des évolutions rencontrées dans le processus de mise en œuvre du présent règlement.	5. La Commission est habilitée à adopter des actes délégués conformément à l'article 50 pour compléter le présent règlement aux fins d'inclure les éléments requis dans la documentation technique figurant à l'annexe V pour tenir compte des progrès techniques ainsi que des évolutions rencontrées dans le processus de mise en œuvre du présent règlement. ***La Commission s'efforce de réduire au minimum la charge administrative pour les micro, petites et moyennes entreprises.***

Amendement 118

Proposition de règlement
Article 24 – paragraphe 1 – point c bis (nouveau)

Texte proposé par la Commission	*Amendement*
	c bis) un schéma européen de certification de cybersécurité adopté conformément à l'article 18, paragraphe 4, du règlement (UE) 2019/881.

Amendement 119

Proposition de règlement
Article 24 – paragraphe 3 – point b

Texte proposé par la Commission	*Amendement*
b) l'évaluation de la conformité sur la base de l'assurance complète de la qualité (module H) prévue à l'annexe VI**.**	b) l'évaluation de la conformité sur la base de l'assurance complète de la qualité (module H) prévue à l'annexe VI***; ou***

Amendement 120

Proposition de règlement
Article 24 – paragraphe 3 – point b bis (nouveau)

Texte proposé par la Commission	*Amendement*
	b bis) le cas échéant, un schéma européen de certification de cybersécurité à un niveau d'assurance «substantiel» ou «élevé» conformément au règlement (UE) 2019/881.

Amendement 121

Proposition de règlement
Article 24 – paragraphe 4 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	4 bis. Pour les produits auxquels s'applique la législation d'harmonisation de l'Union fondée sur le nouveau cadre législatif, le fabricant procède à l'évaluation de la conformité selon les modalités requises par ces actes juridiques. Les exigences énoncées au chapitre III s'appliquent à ces produits.

Amendement 122

Proposition de règlement
Article 24 – paragraphe 5

Texte proposé par la Commission	*Amendement*
5. Les organismes notifiés tiennent compte des intérêts et besoins spécifiques	5. Les organismes notifiés tiennent compte des intérêts et besoins spécifiques

des petites et moyennes entreprises ***(PME)*** lorsqu'ils fixent les redevances imposées pour les procédures d'évaluation de la conformité, et les réduisent proportionnellement auxdits intérêts et besoins spécifiques.	des ***micro,*** petites et moyennes entreprises lorsqu'ils fixent les redevances imposées pour les procédures d'évaluation de la conformité, et les réduisent proportionnellement auxdits intérêts et besoins spécifiques. ***La Commission prend des mesures visant à garantir des procédures plus accessibles et plus abordables et un soutien financier approprié dans le cadre des programmes de l'Union existants, en particulier afin d'alléger la charge pesant sur les micro, petites et moyennes entreprises.***

Amendement 123

Proposition de règlement
Article 24 – paragraphe 5 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	5 bis. Pour les produits comportant des éléments numériques relevant du champ d'application du présent règlement et mis sur le marché ou mis en service par des établissements de crédit régis par la directive 2013/36/UE, l'évaluation de la conformité est effectuée dans le cadre de la procédure visée aux articles 97 à 101 de ladite directive.

Amendement 124

Proposition de règlement
Article 24 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	Article 24 bis
	Lorsque les produits comportant des éléments numériques sont dotés d'un matériel ou d'un logiciel équivalent, un modèle de produit peut être représentatif d'une famille de produits aux fins des procédures d'évaluation de la conformité

suivantes:

a) la procédure de contrôle interne (module A) visée à l'annexe VI; ou

b) la procédure d'examen UE de type (module B) prévue à l'annexe VI, suivie de la conformité au type «UE» sur la base du contrôle interne de la production (module C), prévue à l'annexe VI.

Amendement 125

Proposition de règlement
Article 27 – paragraphe 5

Texte proposé par la Commission	*Amendement*
5. Une autorité notifiante garantit la confidentialité des informations qu'elle obtient.	5. Une autorité notifiante garantit la confidentialité des informations***, y compris les droits de propriété intellectuelle, les informations commerciales confidentielles et les secrets d'affaires,*** qu'elle obtient.

Amendement 126

Proposition de règlement
Article 27 – paragraphe 6 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	6 bis. Une autorité notifiante réduit au minimum les formalités administratives et les redevances, particulièrement pour les PME.

Amendement 127

Proposition de règlement
Article 29 – paragraphe 7 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	7 bis. Les États membres et la Commission mettent en place des mesures

	appropriées pour garantir une disponibilité suffisante de personnel qualifié, afin de réduire au minimum les freins aux activités des organismes d'évaluation de la conformité.

Amendement 128

Proposition de règlement
Article 29 – paragraphe 10

Texte proposé par la Commission	*Amendement*
10. Le personnel d'un organisme d'évaluation de la conformité est lié par le secret professionnel pour toutes les informations dont il prend connaissance dans l'exercice de ses fonctions dans le cadre de l'annexe VI ou de toute disposition de droit national lui donnant effet, sauf à l'égard des autorités de surveillance du marché de l'État membre où il exerce ses activités. Les droits de propriété sont protégés. L'organisme d'évaluation de la conformité dispose de procédures documentées garantissant le respect du présent paragraphe.	10. Le personnel d'un organisme d'évaluation de la conformité est lié par le secret professionnel pour toutes les informations dont il prend connaissance dans l'exercice de ses fonctions dans le cadre de l'annexe VI ou de toute disposition de droit national lui donnant effet, sauf à l'égard des autorités de surveillance du marché de l'État membre où il exerce ses activités. Les droits de propriété ***intellectuelle, les informations commerciales confidentielles et les secrets d'affaires*** sont protégés. L'organisme d'évaluation de la conformité dispose de procédures documentées garantissant le respect du présent paragraphe.

Amendement 129

Proposition de règlement
Article 29 – paragraphe 12

Texte proposé par la Commission	*Amendement*
12. Les organismes d'évaluation de la conformité agissent conformément à un ensemble de conditions cohérentes, justes et raisonnables, notamment en tenant compte des intérêts des ***PME*** pour ce qui est des redevances.	12. Les organismes d'évaluation de la conformité agissent conformément à un ensemble de conditions cohérentes, justes et raisonnables ***en conformité avec l'article 37, paragraphe 2***, notamment en tenant compte des intérêts des ***micro, petites et moyennes entreprises*** pour ce qui est des redevances.

Amendement 130

Proposition de règlement
Article 36 – paragraphe 3

Texte proposé par la Commission	*Amendement*
3. La Commission veille à ce que toutes les informations ***sensibles*** obtenues au cours de ses enquêtes soient traitées de manière confidentielle.	3. La Commission veille à ce que toutes les informations***, y compris les droits de propriété intellectuelle, les informations commerciales confidentielles et les secrets d'affaires,*** obtenues au cours de ses enquêtes soient traitées de manière confidentielle.

Amendement 131

Proposition de règlement
Article 37 – paragraphe 2

Texte proposé par la Commission	*Amendement*
2. Les évaluations de la conformité sont effectuées de manière proportionnée, en évitant d'imposer des charges inutiles aux opérateurs économiques. Les organismes d'évaluation de la conformité accomplissent leurs activités en tenant dûment compte de la taille des entreprises, du secteur dans lequel elles exercent leurs activités, de leur structure, du degré de complexité de la technologie du produit en question et de la nature en masse, ou série, du processus de production.	2. Les évaluations de la conformité sont effectuées de manière proportionnée, en évitant d'imposer des charges inutiles aux opérateurs économiques***, avec une attention particulière portée aux PME***. Les organismes d'évaluation de la conformité accomplissent leurs activités en tenant dûment compte de la taille des entreprises, du secteur dans lequel elles exercent leurs activités, de leur structure, du degré de complexité ***et de l'exposition au risque du type et*** de la technologie du produit en question et de la nature en masse, ou série, du processus de production.

Amendement 132

Proposition de règlement
Article 37 – paragraphe 5

Texte proposé par la Commission	*Amendement*
5. Lorsque, au cours du contrôle de la	5. Lorsque, au cours du contrôle de la

conformité faisant suite à la délivrance d'un certificat de conformité, un organisme notifié constate qu'un produit ne respecte plus les exigences définies par le présent règlement, il exige du fabricant qu'il prenne les mesures correctrices appropriées et suspend ou retire le certificat si nécessaire.	conformité faisant suite à la délivrance d'un certificat de conformité, un organisme notifié constate qu'un produit ne respecte plus les exigences définies par le présent règlement, il exige du fabricant qu'il prenne les mesures correctrices appropriées et ***il soumet à des restrictions,*** suspend ou retire le certificat si nécessaire.

Amendement 133

Proposition de règlement
Article 40 – paragraphe 1

Texte proposé par la Commission	*Amendement*
1. La Commission veille à ce qu'une coordination et une coopération appropriées s'établissent entre les organismes notifiés et soient dûment encadrées sous la forme d'un groupe transsectoriel d'organismes notifiés.	1. La Commission veille à ce qu'une coordination et une coopération appropriées s'établissent entre les organismes notifiés***, en tenant compte de la nécessité de réduire les formalités administratives et les redevances,*** et soient dûment encadrées sous la forme d'un groupe transsectoriel d'organismes notifiés.

Amendement 134

Proposition de règlement
Article 40 – paragraphe 2

Texte proposé par la Commission	*Amendement*
2. Les États membres veillent à ce que les organismes qu'ils ont notifiés participent aux travaux de ce groupe, directement ou par l'intermédiaire de représentants désignés.	2. Les États membres veillent à ce que les organismes qu'ils ont notifiés participent aux travaux de ce groupe, directement ou par l'intermédiaire de représentants désignés***, en tenant également compte de la nécessité de réduire les formalités administratives et les redevances***.

Amendement 135

Proposition de règlement
Article 41 – paragraphe 3

Texte proposé par la Commission	*Amendement*
3. Le cas échéant, les autorités de surveillance du marché coopèrent avec les autorités nationales de certification de cybersécurité désignées en vertu de l'article 58 du règlement (UE) 2019/881 et échangent régulièrement des informations. Les autorités de surveillance du marché désignées coopèrent avec l'ENISA en ce qui concerne le contrôle de la mise en œuvre des obligations en matière de communication d'informations prévues à l'article 11 du présent règlement.	3. Le cas échéant, les autorités de surveillance du marché coopèrent avec les autorités nationales de certification de cybersécurité désignées en vertu de l'article 58 du règlement (UE) 2019/881 et échangent régulièrement des informations. Les autorités de surveillance du marché désignées coopèrent ***efficacement*** avec l'ENISA en ce qui concerne le contrôle de la mise en œuvre des obligations en matière de communication d'informations prévues à l'article 11 du présent règlement. ***Les autorités de surveillance du marché peuvent demander à l'ENISA de fournir des conseils techniques sur des questions liées à la mise en œuvre et à l'exécution du présent règlement, y compris au cours des enquêtes menées conformément à l'article 43 lors desquelles les autorités de surveillance du marché peuvent demander à l'ENISA de fournir des évaluations non contraignantes de la conformité des produits comportant des éléments numériques.***

Amendement 136

Proposition de règlement
Article 41 – paragraphe 7

Texte proposé par la Commission	*Amendement*
7. La Commission facilite les échanges d'expériences entre les autorités de surveillance du marché désignées.	7. La Commission facilite les échanges d'expériences ***réguliers et structurés*** entre les autorités de surveillance du marché désignées***, notamment à l'aide d'un groupe de coopération administrative (ADCO) spécifique institué en vertu du paragraphe 11 du présent article***.

Amendement 137

Proposition de règlement
Article 41 – paragraphe 8

Texte proposé par la Commission	*Amendement*
8. ***Avec le soutien de la Commission, les autorités de surveillance du marché peuvent fournir des orientations et*** des ***conseils aux opérateurs économiques*** sur la mise en œuvre du présent règlement.	8. ***La Commission adopte des lignes directrices et fournit des conseils aux opérateurs économiques, en particulier à ceux qui sont considérés comme*** des ***PME, y compris les microentreprises,*** sur la mise en œuvre du présent règlement. ***Ces lignes directrices et ces conseils visent en particulier à simplifier et à limiter la charge administrative et financière, tout en garantissant une application efficace et cohérente conformément à l'objectif général consistant à garantir la sécurité des produits et la protection des consommateurs.***

Amendement 138

Proposition de règlement
Article 41 – paragraphe 8 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	8 bis. Les autorités de surveillance du marché ont les capacités de recevoir les réclamations des consommateurs conformément à l'article 11 du règlement 2019/1020 notamment en établissant des mécanismes clairs et accessibles afin de faciliter le signalement des vulnérabilités, des incidents et des cybermenaces.

Amendement 139

Proposition de règlement
Article 41 – paragraphe 11

Texte proposé par la Commission	*Amendement*
11. Un groupe de coopération administrative (ADCO) spécifique est établi pour l'application uniforme du présent règlement, conformément à l'article 30, paragraphe 2, du règlement (UE) 2019/1020. Cet ADCO se compose de représentants des autorités de surveillance du marché désignées et, si nécessaire, de représentants des bureaux de liaison uniques.	11. Un groupe de coopération administrative (ADCO) spécifique est établi pour l'application uniforme du présent règlement, ***afin de faciliter la coopération structurée en lien avec la mise en œuvre du présent règlement et de rationaliser les pratiques des autorités de surveillance du marché au sein de l'Union,*** conformément à l'article 30, paragraphe 2, du règlement (UE) 2019/1020. Cet ADCO ***est chargé, en particulier, des missions visées à l'article 32, paragraphe 2, du règlement (UE) 2019/1020, et*** se compose de représentants des autorités de surveillance du marché désignées***, de l'ENISA*** et, si nécessaire, de représentants des bureaux de liaison uniques. ***L'ADCO se réunit à intervalles réguliers et, le cas échéant, sur demande motivée de la Commission, de l'ENISA ou d'un État membre, coordonne son action avec d'autres activités existantes de l'Union liées à la surveillance du marché et à la sécurité des consommateurs et, le cas échéant, coopère et échange des informations avec d'autres réseaux, groupes et organismes de l'Union. L'ADCO peut inviter des spécialistes et d'autres tiers, notamment des organisations de consommateurs, à assister à ses réunions.***

Amendement 140

Proposition de règlement
Article 41 – paragraphe 11 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	11 bis. Pour les produits comportant des éléments numériques qui relèvent du champ d'application du présent règlement, distribués, mis en service ou utilisés par des établissements financiers

	régis par la législation pertinente de l'Union sur les services financiers, l'autorité de surveillance du marché, aux fins du présent règlement, est l'autorité compétente responsable de la supervision financière de ces établissements en vertu de ladite législation.

Amendement 141

Proposition de règlement
Article 42 – alinéa 1

Texte proposé par la Commission	*Amendement*
Lorsque cela est nécessaire pour évaluer la conformité des produits comportant des éléments numériques et des processus mis en place par leurs fabricants aux exigences essentielles énoncées à l'annexe I, et sur demande motivée, les autorités de surveillance du marché ont accès aux données requises pour évaluer la conception, le développement, la production et le traitement des vulnérabilités de ces produits, y compris la documentation interne correspondante de l'opérateur économique concerné.	Lorsque cela est nécessaire pour évaluer la conformité des produits comportant des éléments numériques et des processus mis en place par leurs fabricants aux exigences essentielles énoncées à l'annexe I, et sur demande motivée, les autorités de surveillance du marché ont accès aux données requises pour évaluer la conception, le développement, la production et le traitement des vulnérabilités de ces produits, y compris la documentation interne correspondante de l'opérateur économique concerné. ***Le cas échéant, et conformément à l'article 52, paragraphe 1, point a), cette opération est réalisée dans un environnement sûr et contrôlé, défini par le fabricant.***

Amendement 142

Proposition de règlement
Article 43 – paragraphe 1 – alinéa 2

Texte proposé par la Commission	*Amendement*
Si, au cours de cette évaluation, l'autorité de surveillance du marché constate que le produit comportant des éléments numériques ne respecte pas les exigences énoncées dans le présent règlement, elle invite sans tarder l'opérateur économique	Si, au cours de cette évaluation, l'autorité de surveillance du marché constate que le produit comportant des éléments numériques ne respecte pas les exigences énoncées dans le présent règlement ***ou présente une menace pour la sécurité***

en cause à prendre toutes les mesures correctives appropriées pour mettre le produit en conformité avec ces exigences, le retirer du marché ou le rappeler dans un délai raisonnable, proportionné à la nature du risque, qu'elle prescrit.	***nationale***, elle invite sans tarder l'opérateur économique en cause à prendre toutes les mesures correctives appropriées pour mettre le produit en conformité avec ces exigences, le retirer du marché ou le rappeler dans un délai raisonnable, proportionné à la nature du risque, qu'elle prescrit. ***Avant de procéder à l'évaluation susmentionnée, l'autorité de surveillance du marché peut, si nécessaire, compte tenu de l'importance du risque de cybersécurité, demander à l'opérateur concerné de suspendre ou restreindre immédiatement la disponibilité du produit sur le marché pendant la durée de ladite évaluation.***

Amendement 143

Proposition de règlement
Article 43 – paragraphe 4 – alinéa 1

Texte proposé par la Commission	*Amendement*
Lorsque le fabricant d'un produit comportant des éléments numériques ne prend pas les mesures correctives adéquates dans le délai visé au paragraphe 1, deuxième alinéa, l'autorité de surveillance du marché adopte toutes les mesures provisoires appropriées pour interdire ou restreindre la mise à disposition du produit sur son marché national ou pour procéder à son retrait de ce marché ou à son rappel.	Lorsque le fabricant d'un produit comportant des éléments numériques ne prend pas les mesures correctives adéquates dans le délai visé au paragraphe 1, deuxième alinéa, ***ou si l'autorité compétente de l'État membre considère que le produit présente une menace pour la sécurité nationale,*** l'autorité de surveillance du marché adopte toutes les mesures provisoires appropriées pour interdire ou restreindre la mise à disposition du produit sur son marché national ou pour procéder à son retrait de ce marché ou à son rappel.

Amendement 144

Proposition de règlement
Article 45 – paragraphe 1

Texte proposé par la Commission	*Amendement*
1. Lorsque la Commission a des raisons suffisantes de considérer, y compris sur la base des informations fournies par l'ENISA, qu'un produit comportant des éléments numériques présentant un risque de cybersécurité important n'est pas conforme aux exigences énoncées dans le présent règlement, elle ***peut demander*** aux autorités de surveillance du marché concernées de procéder à une évaluation de la conformité et de suivre les procédures visées à l'article 43.	1. Lorsque la Commission a des raisons suffisantes de considérer, y compris sur la base des informations fournies par ***les autorités compétentes des États membres, les centres de réponse aux incidents de sécurité informatique (CSIRT) désignés ou établis conformément à la directive (UE) 2022/2555 ou*** l'ENISA, qu'un produit comportant des éléments numériques présentant un risque de cybersécurité important n'est pas conforme aux exigences énoncées dans le présent règlement, elle ***demande*** aux autorités de surveillance du marché concernées de procéder à une évaluation de la conformité et de suivre les procédures visées à l'article 43.

Amendement 145

Proposition de règlement
Article 45 – paragraphe 2

Texte proposé par la Commission	*Amendement*
2. Dans des circonstances ***exceptionnelles*** qui justifient une intervention immédiate pour préserver le bon fonctionnement du marché intérieur et lorsque la Commission a des raisons ***suffisantes*** de considérer que le produit visé au paragraphe 1 demeure non conforme aux exigences énoncées dans le présent règlement et qu'aucune mesure effective n'a été prise par les autorités de surveillance du marché concernées, la Commission ***peut demander*** à l'ENISA de procéder à une évaluation de la conformité. La Commission en informe les autorités de surveillance du marché concernées. Les opérateurs économiques concernés coopèrent comme il se doit avec l'ENISA.	2. Dans des circonstances qui justifient une intervention immédiate pour préserver le bon fonctionnement du marché intérieur et lorsque la Commission a des raisons de considérer que le produit visé au paragraphe 1 demeure non conforme aux exigences énoncées dans le présent règlement et qu'aucune mesure effective n'a été prise par les autorités de surveillance du marché concernées, la Commission ***demande*** à l'ENISA de procéder à une évaluation de la conformité. La Commission en informe les autorités de surveillance du marché concernées. Les opérateurs économiques concernés coopèrent comme il se doit avec l'ENISA.

Amendement 146

Proposition de règlement
Article 46 – paragraphe 1

Texte proposé par la Commission	*Amendement*
1. Lorsque, après avoir réalisé une évaluation au titre de l'article 43, l'autorité de surveillance du marché d'un État membre constate que, bien qu'un produit comportant des éléments numériques et les processus mis en place par le fabricant soient conformes au présent règlement, ils présentent un risque de cybersécurité important ainsi qu'un risque pour la santé ou la sécurité des personnes, pour le respect des obligations découlant du droit de l'Union ou du droit national visant à protéger les droits fondamentaux, pour la disponibilité, l'authenticité, l'intégrité ou la confidentialité des services proposés au moyen d'un système d'information électronique par des entités essentielles du type visé à ***[l'annexe*** I de la directive ***XXX/XXXX*** (***NIS***2)***]*** ou pour d'autres aspects de la protection de l'intérêt public, elle exige de l'opérateur concerné qu'il prenne toutes les mesures appropriées pour faire en sorte qu'une fois mis sur le marché, le produit comportant des éléments numériques et les processus mis en place par le fabricant concerné ne présentent plus ce risque, pour retirer ledit produit du marché ou pour le rappeler dans un délai raisonnable, proportionné à la nature du risque.	1. Lorsque, après avoir réalisé une évaluation au titre de l'article 43, l'autorité de surveillance du marché d'un État membre constate que, bien qu'un produit comportant des éléments numériques et les processus mis en place par le fabricant soient conformes au présent règlement, ils présentent un risque de cybersécurité important ainsi qu'un risque pour la santé ou la sécurité des personnes, pour le respect des obligations découlant du droit de l'Union ou du droit national visant à protéger les droits fondamentaux, pour la disponibilité, l'authenticité, l'intégrité ou la confidentialité des services proposés au moyen d'un système d'information électronique par des entités essentielles du type visé à ***l'annexe*** I de la directive ***(UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) nº 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (directive SRI*** 2) ou pour d'autres aspects de la protection de l'intérêt public, elle exige de l'opérateur ***économique*** concerné qu'il prenne toutes les mesures appropriées pour faire en sorte qu'une fois mis sur le marché, le produit comportant des éléments numériques et les processus mis en place par le fabricant concerné ne présentent plus ce risque, pour retirer ledit produit du marché ou pour le rappeler dans un délai raisonnable, proportionné à la nature du risque.

Amendement 147

Proposition de règlement
Article 46 – paragraphe 2

Texte proposé par la Commission	*Amendement*
2. Le fabricant ou les autres opérateurs concernés s'assurent que des mesures correctives sont prises pour tous les produits comportant des éléments numériques concernés qu'ils ont mis à disposition sur le marché dans toute l'Union dans le délai établi par l'autorité de surveillance du marché de l'État membre visée au paragraphe 1.	2. Le fabricant ou les autres opérateurs ***économiques*** concernés s'assurent que des mesures correctives sont prises pour tous les produits comportant des éléments numériques concernés qu'ils ont mis à disposition sur le marché dans toute l'Union dans le délai établi par l'autorité de surveillance du marché de l'État membre visée au paragraphe 1.

Amendement 148

Proposition de règlement
Article 46 – paragraphe 6

Texte proposé par la Commission	*Amendement*
6. Lorsque la Commission a des raisons suffisantes de considérer, y compris sur la base des informations fournies par l'ENISA, qu'un produit comportant des éléments numériques, bien que conforme au présent règlement, présente les risques visés au paragraphe 1, elle ***peut demander*** aux autorités de surveillance du marché concernées de procéder à une évaluation de la conformité et de suivre les procédures visées à l'article 43 et aux paragraphes 1, 2 et 3 du présent article.	6. Lorsque la Commission a des raisons suffisantes de considérer, y compris sur la base des informations fournies par l'ENISA, qu'un produit comportant des éléments numériques, bien que conforme au présent règlement, présente les risques visés au paragraphe 1, elle ***demande*** aux autorités de surveillance du marché concernées de procéder à une évaluation de la conformité et de suivre les procédures visées à l'article 43 et aux paragraphes 1, 2 et 3 du présent article.

Amendement 149

Proposition de règlement
Article 46 – paragraphe 7

Texte proposé par la Commission	*Amendement*
7. Dans des circonstances ***exceptionnelles*** qui justifient une intervention immédiate pour préserver le bon fonctionnement du marché intérieur et	7. Dans des circonstances qui justifient une intervention immédiate pour préserver le bon fonctionnement du marché intérieur et lorsque la Commission a des

lorsque la Commission a des raisons suffisantes de considérer que le produit visé au paragraphe 6 continue de présenter les risques visés au paragraphe 1 et qu'aucune mesure effective n'a été prise par les autorités nationales de surveillance du marché concernées, la Commission ***peut demander*** à l'ENISA de procéder à une évaluation des risques présentés par ledit produit et en informe les autorités de surveillance du marché concernées. Les opérateurs économiques concernés coopèrent comme il se doit avec l'ENISA.

raisons suffisantes de considérer que le produit visé au paragraphe 6 continue de présenter les risques visés au paragraphe 1 et qu'aucune mesure effective n'a été prise par les autorités nationales de surveillance du marché concernées, la Commission ***demande*** à l'ENISA de procéder à une évaluation des risques présentés par ledit produit et en informe les autorités de surveillance du marché concernées. Les opérateurs économiques concernés coopèrent comme il se doit avec l'ENISA.

Amendement 150

Proposition de règlement
Article 48 – paragraphe 1

Texte proposé par la Commission	*Amendement*
1. Les autorités de surveillance du marché ***peuvent convenir*** avec d'autres autorités compétentes ***de mener des activités conjointes visant*** à garantir la cybersécurité et la protection des consommateurs en ce qui concerne des produits spécifiques comportant des éléments numériques mis sur le marché ou mis à disposition sur le marché, en particulier des produits dont il est souvent constaté qu'ils présentent des risques de cybersécurité.	1. Les autorités de surveillance du marché ***mènent régulièrement des activités conjointes*** avec d'autres autorités compétentes***, qui visent*** à garantir la cybersécurité et la protection des consommateurs en ce qui concerne des produits spécifiques comportant des éléments numériques mis sur le marché ou mis à disposition sur le marché, en particulier des produits dont il est souvent constaté qu'ils présentent des risques de cybersécurité. ***Ces activités comprennent des inspections des produits acquis sous une fausse identité.***

Amendement 151

Proposition de règlement
Article 48 – paragraphe 2

Texte proposé par la Commission	*Amendement*
2. La Commission ou l'ENISA ***peuvent proposer*** des activités conjointes de contrôle du respect du présent règlement	2. La Commission ou l'ENISA ***proposent*** des activités conjointes de contrôle du respect du présent règlement à

à mener par les autorités de surveillance du marché sur la base d'indications ou d'informations relatives à une non-conformité potentielle, dans plusieurs États membres, de produits relevant du champ d'application du présent règlement, aux exigences fixées par ce dernier.

mener par les autorités de surveillance du marché sur la base d'indications ou d'informations relatives à une non-conformité potentielle, dans plusieurs États membres, de produits relevant du champ d'application du présent règlement, aux exigences fixées par ce dernier.

Amendement 152

Proposition de règlement
Article 49 – paragraphe 1

Texte proposé par la Commission	*Amendement*
1. Les autorités de surveillance du marché ***peuvent décider de mener*** des actions de contrôle coordonnées et simultanées (opérations «coup de balai») concernant certains produits ou catégories de produits comportant des éléments numériques afin de vérifier le respect du présent règlement ou de détecter des infractions à celui-ci.	1. Les autorités de surveillance du marché ***mènent régulièrement*** des actions de contrôle coordonnées et simultanées (opérations «coup de balai») concernant certains produits ou catégories de produits comportant des éléments numériques afin de vérifier le respect du présent règlement ou de détecter des infractions à celui-ci.

Amendement 153

Proposition de règlement
Article 49 – paragraphe 2

Texte proposé par la Commission	*Amendement*
2. Sauf accord contraire des autorités de surveillance du marché participantes, les opérations «coup de balai» sont coordonnées par la Commission. Le coordonnateur de l'opération «coup de balai» ***peut***, s'il y a lieu, ***publier*** les résultats agrégés de l'opération.	2. Sauf accord contraire des autorités de surveillance du marché participantes, les opérations «coup de balai» sont coordonnées par la Commission. Le coordonnateur de l'opération «coup de balai» ***publie***, s'il y a lieu, les résultats agrégés de l'opération.

Amendement 154

Proposition de règlement
Article 49 – paragraphe 3

Texte proposé par la Commission	*Amendement*
3. L'ENISA ***peut identifier***, dans l'exécution de ses tâches, y compris sur la base des notifications reçues conformément à l'article 11, paragraphes 1 et 2, des catégories de produits pour lesquelles des opérations «coup de balai» ***peuvent être*** organisées. La proposition d'opération «coup de balai» est soumise au coordonnateur potentiel visé au paragraphe 2 pour examen par les autorités de surveillance du marché.	3. L'ENISA ***identifie***, dans l'exécution de ses tâches, y compris sur la base des notifications reçues conformément à l'article 11, paragraphes 1 et 2, des catégories de produits pour lesquelles des opérations «coup de balai» ***sont*** organisées. La proposition d'opération «coup de balai» est soumise au coordonnateur potentiel visé au paragraphe 2 pour examen par les autorités de surveillance du marché.

Amendement 155

Proposition de règlement
Article 49 – paragraphe 5

Texte proposé par la Commission	*Amendement*
5. Les autorités de surveillance du marché ***peuvent inviter*** des fonctionnaires de la Commission et d'autres personnes les accompagnant habilitées par la Commission à participer aux opérations «coup de balai».	5. Les autorités de surveillance du marché ***invitent*** des fonctionnaires de la Commission et d'autres personnes les accompagnant habilitées par la Commission à participer aux opérations «coup de balai».

Amendement 156

Proposition de règlement
Article 9 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	Article 49 bis
	Fourniture de conseils techniques
	1. La Commission nomme, par un acte d'exécution, un groupe d'experts chargé de fournir des conseils techniques aux autorités de surveillance du marché sur des questions liées à la mise en œuvre et à l'exécution du présent règlement. L'acte d'exécution précise, entre autres, les détails liés à la composition du groupe,

à son fonctionnement et à la rémunération de ses membres. En particulier, le groupe d'experts fournit des évaluations non contraignantes de produits comportant des éléments numériques, sur demande d'une autorité de surveillance du marché qui mène une enquête en vertu de l'article 43, et de la liste de produits critiques comportant des éléments numériques figurant à l'annexe II, ainsi que sur la nécessité éventuelle de la mettre à jour.

2. Le groupe d'experts se compose d'experts indépendants nommés pour un mandat de trois ans renouvelable par la Commission sur la base de leur expertise scientifique ou technique dans le domaine.

3. La Commission nomme un nombre d'experts jugé suffisant pour répondre aux besoins prévus.

4. La Commission prend les mesures nécessaires pour gérer et prévenir tout conflit d'intérêts. Les déclarations d'intérêts des membres du groupe d'experts sont rendues publiques.

5. Les experts nommés s'acquittent de leurs tâches avec le plus haut niveau de professionnalisme, d'indépendance, d'impartialité et d'objectivité.

6. Lors de l'adoption de positions, d'avis et de rapports, le groupe d'experts s'efforce de parvenir à un consensus. En l'absence de consensus, les décisions sont prises à la majorité simple des membres du groupe.

Amendement 157

Proposition de règlement
Article 53 – paragraphe 1

Texte proposé par la Commission	*Amendement*
1. Les États membres déterminent le	1. Les États membres déterminent le

régime des sanctions applicables aux violations du présent règlement par les opérateurs économiques et prennent toutes les mesures nécessaires pour assurer la mise en œuvre de ces sanctions. Les sanctions prévues sont effectives, proportionnées et dissuasives.	régime des sanctions applicables aux violations du présent règlement par les opérateurs économiques et prennent toutes les mesures nécessaires pour assurer la mise en œuvre de ces sanctions. Les sanctions prévues sont effectives, proportionnées et dissuasives ***et tiennent compte des spécificités des micro, petites et moyennes entreprises***.

Amendement 158

Proposition de règlement
Article 53 – paragraphe 6 – point a bis (nouveau)

Texte proposé par la Commission	*Amendement*
	a bis) le point de savoir si l'infraction est involontaire;

Amendement 159

Proposition de règlement
Article 53 – paragraphe 6 – point b

Texte proposé par la Commission	*Amendement*
b) la question de savoir si des amendes administratives ont déjà été imposées par d'autres autorités de surveillance du marché au même opérateur pour une infraction similaire;	b) la question de savoir si des amendes administratives ont déjà été imposées par ***les mêmes ou*** d'autres autorités de surveillance du marché au même opérateur pour une infraction similaire;

Amendement 160

Proposition de règlement
Article 53 – paragraphe 6 – point c

Texte proposé par la Commission	*Amendement*
c) la taille et la part de marché de l'opérateur qui commet l'infraction**.**	c) la taille et la part de marché de l'opérateur qui commet l'infraction**,** ***compte tenu de l'ampleur des risques, des conséquences et des spécificités***

financières des micro, petites et moyennes entreprises;

Amendement 161

Proposition de règlement
Article 53 – paragraphe 6 – point c bis (nouveau)

Texte proposé par la Commission	*Amendement*
	c bis) le comportement de l'opérateur une fois qu'il a été informé ou qu'il a pris connaissance de la non-conformité en question, y compris la question de savoir si l'opérateur, lorsqu'il a pris connaissance de la non-conformité, a appliqué toutes les mesures correctives appropriées ainsi que les mesures raisonnablement nécessaires pour éviter ou réduire au minimum d'éventuelles conséquences négatives.

Amendement 162

Proposition de règlement
Chapitre VII bis (nouveau)

Texte proposé par la Commission	*Amendement*
	MESURES DE SOUTIEN À L'INNOVATION

Amendement 163

Proposition de règlement
Article 53 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	Article 53 bis
	Sas réglementaires
	La Commission et l'ENISA peuvent établir un sas réglementaire européen avec la participation volontaire de

	fabricants de produits comportant des éléments numériques afin:
	a) de ménager un environnement contrôlé qui facilite la mise au point, l'expérimentation et la validation de la conception, du développement et de la fabrication de produits comportant des éléments numériques, avant leur mise sur le marché ou leur mise en service conformément à un plan spécifique;
	b) d'offrir un accompagnement pratique aux opérateurs économiques, y compris au moyen de lignes directrices et de bonnes pratiques afin de satisfaire aux exigences essentielles énoncées à l'annexe I;
	c) de contribuer à l'apprentissage réglementaire fondé sur des données probantes.

Amendement 164

Proposition de règlement
Article 54 – titre

Texte proposé par la Commission	*Amendement*
Modification du règlement (UE) 2019/1020	***Modifications*** du règlement (UE) 2019/1020 ***et de la directive 2020/1828/CE***

Amendement 165

Proposition de règlement
Article 54 – paragraphe 1 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	1 bis. À l'annexe I de la directive 2020/1828/CE, le point suivant est ajouté:
	«67) [Règlement XXX] [législation sur la cyberrésilience].»

Amendement 166

Proposition de règlement
Article 54 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	Article 54 bis
	Règlement délégué (UE) 2022/30
	Le présent règlement est conçu de telle sorte que tous les produits régis par les exigences essentielles établies à l'article 3, paragraphe 3, points d), e) et f), de la directive 2014/53/UE, telles que décrites dans le règlement délégué (UE) 2022/30, soient conformes au présent règlement. Afin de garantir la sécurité juridique, le règlement délégué (UE) 2022/30 est abrogé au moment de l'entrée en vigueur du présent règlement.

Amendement 167

Proposition de règlement
Article 57 – alinéa 2

Texte proposé par la Commission	*Amendement*
Il est applicable à partir du [***24*** mois après la date d'entrée en vigueur du présent règlement]. ***Cependant***, ***l'article 11 s'applique à compter du [12*** mois après la date ***d'entrée en vigueur*** du présent règlement].	Il est applicable à partir du [***36*** mois après la date d'entrée en vigueur du présent règlement]. ***En ce qui concerne les produits comportant des éléments critiques***, ***les chapitres II, III, V et VII s'appliquent au plus tôt le [20*** mois après la date ***de publication des normes harmonisées élaborées dans le cadre de la normalisation requise aux fins*** du présent règlement]. ***Au plus tard six mois après la date d'entrée en vigueur du présent règlement, la Commission publie des lignes directrices relatives aux modalités d'application des exigences prévues par le présent règlement pour les produits immatériels.***

Amendement 168

Proposition de règlement
Annexe I – partie 1 – point 3 – partie introductive

Texte proposé par la Commission	*Amendement*
3) Sur la base de l'évaluation des risques visée à l'article 10, paragraphe 2, les produits comportant des éléments numériques doivent, le cas échéant:	3) Sur la base de l'évaluation des risques ***de cybersécurité*** visée à l'article 10, paragraphe 2, les produits comportant des éléments numériques doivent, le cas échéant:

Amendement 169

Proposition de règlement
Annexe I – partie 1 – point 3 – sous-point -a (nouveau)

Texte proposé par la Commission	*Amendement*
	-a) être mis sur le marché sans aucune vulnérabilité exploitable connue à l'égard d'un dispositif ou réseau extérieur;

Amendement 170

Proposition de règlement
Annexe I – partie 1 – point 3 – sous-point a

Texte proposé par la Commission	*Amendement*
a) être livrés avec une configuration de sécurité par défaut***, y compris la possibilité de réinitialiser le produit à son état d'origine***;	a) être livrés avec une configuration de sécurité par défaut;

Amendement 171

Proposition de règlement
Annexe I – partie 1 – point 3 – point c

Texte proposé par la Commission	*Amendement*
c) protéger la confidentialité des	c) protéger la confidentialité des

données stockées, transmises ou traitées de toute autre manière, à caractère personnel ou autres, par exemple ***en chiffrant les*** données pertinentes au repos ou en transit au moyen de mécanismes de pointe;	données stockées, transmises ou traitées de toute autre manière, à caractère personnel ou autres, par exemple ***grâce au chiffrement, à la tokénisation, au contrôle compensatoire et à toute autre protection appropriée des*** données pertinentes au repos ou en transit au moyen de mécanismes de pointe;

Amendement 172

Proposition de règlement
Annexe I – partie 1 – point 3 – point d

Texte proposé par la Commission	*Amendement*
d) protéger l'intégrité des données stockées, transmises ou traitées de toute autre manière, à caractère personnel ou autres, des commandes, des programmes et de la configuration contre toute manipulation ou modification non autorisée par l'utilisateur, ainsi que signaler les corruptions;	d) protéger l'intégrité des données stockées, transmises ou traitées de toute autre manière, à caractère personnel ou autres, des commandes, des programmes et de la configuration contre toute manipulation ou modification non autorisée par l'utilisateur, ainsi que signaler les corruptions ***ou tout accès non autorisé potentiel***;

Amendement 173

Proposition de règlement
Annexe I – partie 1 – point 3 – sous-point f

Texte proposé par la Commission	*Amendement*
f) protéger la disponibilité des fonctions essentielles, y compris la résilience et l'atténuation des attaques par déni de service;	f) protéger la disponibilité des fonctions essentielles ***et des fonctions de base***, y compris la résilience et l'atténuation des attaques par déni de service;

Amendement 174

Proposition de règlement
Annexe I – partie 1 – point 3 – sous-point i

Texte proposé par la Commission	*Amendement*
i) être conçus, développés et fabriqués de manière à réduire les conséquences d'un incident, en utilisant des mécanismes et des techniques appropriés de limitation de l'exploitation de failles;	i) être conçus, développés et fabriqués de manière à réduire les conséquences d'un incident ***important***, en utilisant des mécanismes et des techniques appropriés de limitation de l'exploitation de failles;

Amendement 175

Proposition de règlement
Annexe I – partie 1 – point 3 – sous-point j

Texte proposé par la Commission	*Amendement*
j) fournir des informations relatives à la sécurité en ***enregistrant*** et/ou ***en surveillant*** les activités internes pertinentes, y compris l'accès ou la modification des données, des services ou des fonctions;	j) fournir des informations relatives à la sécurité en ***communiquant, sur demande de l'utilisateur, les capacités d'enregistrement*** et/ou ***de surveillance, localement et au niveau du dispositif pour*** les activités internes pertinentes, y compris l'accès ou la modification des données, des services ou des fonctions;

Amendement 176

Proposition de règlement
Annexe I – partie 1 – point 3 – sous-point k

Texte proposé par la Commission	*Amendement*
k) garantir que les vulnérabilités puissent être traitées par des mises à jour de sécurité, y compris, le cas échéant, par des mises à jour automatiques et la notification des mises à jour disponibles aux utilisateurs***.***	k) garantir que les vulnérabilités puissent être traitées par des mises à jour de sécurité, y compris, le cas échéant, ***distinctes des mises à jour de fonctionnalités, et*** par des mises à jour automatiques et la notification des mises à jour disponibles aux utilisateurs***;***

Amendement 177

Proposition de règlement
Annexe I – partie 1 – point 3 – sous-point k bis (nouveau)

Texte proposé par la Commission	*Amendement*
	k bis) être conçus, élaborés et fabriqués de manière à permettre leur abandon sécurisé et leur recyclage éventuel lorsqu'ils parviennent à la fin de leur cycle de vie, notamment en permettant aux utilisateurs de se retirer et de supprimer de manière sécurisée toutes les données, et ce de manière permanente.

Amendement 178

Proposition de règlement
Annexe I – partie 2 – alinéa 1 – point 2

Texte proposé par la Commission	*Amendement*
2) s'agissant des risques posés aux produits comportant des éléments numériques, gérer et corriger sans délai les vulnérabilités, notamment en fournissant des mises à jour de sécurité;	2) s'agissant des risques posés aux produits comportant des éléments numériques, gérer et corriger sans délai les vulnérabilités ***critiques et élevées***, notamment en fournissant des mises à jour de sécurité ***ou en consignant les motifs de non-correction des vulnérabilités***;

Amendement 179

Proposition de règlement
Annexe I – partie 2 – alinéa 1 – point 4

Texte proposé par la Commission	*Amendement*
4) dès la publication d'une mise à jour de sécurité, divulguer publiquement des informations sur les vulnérabilités corrigées, en ce compris une description des vulnérabilités, des informations permettant aux utilisateurs d'identifier le produit concerné, les conséquences de ces vulnérabilités, leur gravité et des informations aidant les utilisateurs à y remédier;	4) dès la publication d'une mise à jour de sécurité, divulguer publiquement ***ou conformément aux bonnes pratiques du secteur*** des informations sur les vulnérabilités ***connues*** corrigées, en ce compris une description des vulnérabilités, des informations permettant aux utilisateurs d'identifier le produit concerné, les conséquences de ces vulnérabilités, leur gravité et des informations ***claires et accessibles*** aidant les utilisateurs à y remédier;

Amendement 180

Proposition de règlement
Annexe I – partie 2 – paragraphe 1 – point 4 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	4 bis) partager et divulguer des informations concernant les corrections et les vulnérabilités de manière contrôlée, en respectant les principes de «réduction des risques» et les secrets d'affaires au moyen d'une divulgation responsable des vulnérabilités aux acteurs qui peuvent agir pour atténuer la vulnérabilité, et qui ne sont pas rendues publiques afin d'éviter le risque d'informer par inadvertance d'éventuelles personnes malveillantes;

Amendement 181

Proposition de règlement
Annexe I – partie 2 – alinéa 1 – point 7

Texte proposé par la Commission	*Amendement*
7) prévoir des mécanismes de distribution sécurisée des mises à jour pour les produits comportant des éléments numériques afin de s'assurer que les vulnérabilités exploitables soient corrigées ou atténuées rapidement;	7) prévoir des mécanismes de distribution sécurisée des mises à jour ***de sécurité*** pour les produits comportant des éléments numériques afin de s'assurer que les vulnérabilités exploitables soient corrigées ou atténuées rapidement;

Amendement 182

Proposition de règlement
Annexe I – partie 2 – alinéa 1 – point 8

Texte proposé par la Commission	*Amendement*
8) veiller à ce que, lorsque des correctifs ou des mises à jour de sécurité ***sont disponibles*** pour remédier à des problèmes de sécurité constatés, ***ils*** soient	8) veiller à ce que, lorsque des correctifs ou des mises à jour de sécurité ***peuvent raisonnablement être mises à disposition*** pour remédier à des problèmes

diffusés sans délai et gratuitement, et accompagnés de messages de recommandation fournissant aux utilisateurs les informations pertinentes, notamment sur les éventuelles mesures à prendre.	de sécurité constatés, ***les moyens par lesquels les utilisateurs peuvent les obtenir*** soient diffusés sans délai et gratuitement ***ou à un coût transparent et non discriminatoire***, et accompagnés de messages de recommandation fournissant aux utilisateurs les informations pertinentes, notamment sur les éventuelles mesures à prendre.

Amendement 183

Proposition de règlement
Annexe II – alinéa 1 – point 2

Texte proposé par la Commission	*Amendement*
2) le point de contact où les informations sur les vulnérabilités du produit en matière de cybersécurité peuvent être signalées et reçues;	2) le point de contact ***unique*** où les informations sur les vulnérabilités du produit en matière de cybersécurité peuvent être signalées et reçues;

Amendement 184

Proposition de règlement
Annexe II – alinéa 1 – point 5

Texte proposé par la Commission	*Amendement*
5) toutes circonstances connues ou prévisibles liées à l'utilisation du produit comportant des éléments numériques conformément à son utilisation prévue ou dans des conditions de mauvaise utilisation raisonnablement prévisible, susceptibles d'entraîner des risques de cybersécurité importants;	***supprimé***

Amendement 185

Proposition de règlement
Annexe II – alinéa 1 – point 6

Texte proposé par la Commission	*Amendement*
6) le cas échéant, l'endroit où la nomenclature des logiciels peut être consultée;	6) le cas échéant, l'endroit où la nomenclature des logiciels peut être consultée ***par les autorités compétentes***;

Amendement 186

Proposition de règlement
Annexe II – alinéa 1 – point 8

Texte proposé par la Commission	*Amendement*
8) le type d'assistance technique en matière de sécurité proposé par le fabricant et la date de fin de celle-ci***, à tout le moins la date jusqu'à laquelle les utilisateurs peuvent s'attendre à recevoir des mises à jour de sécurité***;	8. le type d'assistance technique en matière de sécurité proposé par le fabricant et la date de fin de celle-ci;

Amendement 187

Proposition de règlement
Annexe II – alinéa 1 – point 8 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	8 bis) la date de fin de la durée de vie prévue du produit, clairement indiquée, le cas échéant, sur l'emballage du produit, jusqu'à laquelle le fabricant garantit le traitement efficace des vulnérabilités et la fourniture de mises à jour de sécurité;

Amendement 188

Proposition de règlement
Annexe II – alinéa 1 – point 9 – sous-point a

Texte proposé par la Commission	*Amendement*
a) les mesures nécessaires lors de la mise en service initiale du produit et pendant toute sa durée de vie pour assurer	***supprimé***

sa sécurité d'utilisation,

Amendement 189

Proposition de règlement
Annexe II – alinéa 1 – point 9 – sous-point b

Texte proposé par la Commission	*Amendement*
b) la façon dont les modifications apportées au produit peuvent affecter la sécurité des données,	***supprimé***

Amendement 190

Proposition de règlement
Annexe II – alinéa 1 – point 9 – sous-point c bis (nouveau)

Texte proposé par la Commission	*Amendement*
	c bis) la durée de vie prévue du produit et la date jusqu'à laquelle le fabricant garantit le traitement efficace des vulnérabilités et la fourniture de mises à jour de sécurité;

Amendement 191

Proposition de règlement
Annexe II – alinéa 1 – point 9 – sous-point d

Texte proposé par la Commission	*Amendement*
d) la mise hors service sécurisée du produit, en ce compris des informations sur la manière dont les données utilisateur peuvent être supprimées en toute sécurité.	***supprimé***

Amendement 192

Proposition de règlement
Annexe III – classe I – point 3 bis (nouveau)

Texte proposé par la Commission	*Amendement*
	3 bis) plateformes d'authentification, d'autorisation et de traçabilité (AAA);

Amendement 193

Proposition de règlement
Annexe III – classe I – point 15

Texte proposé par la Commission	*Amendement*
15) interfaces réseau physiques;	15) interfaces réseau physiques ***et virtuelles***;

Amendement 194

Proposition de règlement
Annexe III – classe I – point 18

Texte proposé par la Commission	*Amendement*
18) routeurs, modems destinés à la connexion à l'internet et commutateurs, non couverts par la classe II;	***supprimé***

Amendement 195

Proposition de règlement
Annexe III – classe I – point 23

Texte proposé par la Commission	*Amendement*
23) ***internet industriel*** des objets non couvert par la classe II.	23) ***produits industriels comportant des éléments numériques qui peuvent être désignés comme faisant partie de l'internet*** des objets non couvert par la classe II.

Amendement 196

Proposition de règlement
Annexe III – classe II – point 4

Texte proposé par la Commission	*Amendement*
4) pare-feu, systèmes de détection et/ou de prévention des intrusions destinés à un usage industriel;	4) pare-feu, ***passerelles de sécurité,*** systèmes de détection et/ou de prévention des intrusions destinés à un usage industriel;

Amendement 197

Proposition de règlement
Annexe III – classe II – point 7

Texte proposé par la Commission	*Amendement*
7) routeurs, modems destinés à la connexion à l'internet et ***commutateurs, destinés*** à ***un usage industriel***;	7. routeurs, modems destinés à la connexion à l'internet***, commutateurs*** et ***autres nœuds de réseau nécessaires*** à ***la fourniture du service de connectivité***;

Amendement 198

Proposition de règlement
Annexe IV bis (nouveau)

Texte proposé par la Commission	*Amendement*
	ANNEXE IV bis
	DÉCLARATION UE D'INCORPORATON POUR LES QUASI-PRODUITS COMPORTANT DES ÉLÉMENTS NUMÉRIQUES
	La déclaration UE d'incorporation pour les quasi-produits comportant des éléments numériques prévue à l'article 20 bis contient l'ensemble des informations suivantes:
	1. nom et type, ainsi que toute information supplémentaire permettant l'identification unique du quasi-produit comportant des éléments numériques;
	2. objet de la déclaration (identification du quasi-produit permettant sa traçabilité; au besoin, une

	photographie peut être jointe);
	3. une mention indiquant que le quasi-produit décrit ci-dessus est conforme à la législation d'harmonisation de l'Union applicable;
	4. les références de tout acte de l'Union pertinent concerné, y compris ses références de publication;
	5. informations supplémentaires:
	Signé par et au nom de:
	……
	(date et lieu d'établissement):
	(nom, fonction) (signature):

Amendement 199

Proposition de règlement
Annexe V – alinéa 1 – point 1 – sous-point a

Texte proposé par la Commission	*Amendement*
a) l'utilisation prévue;	***supprimé***

Amendement 200

Proposition de règlement
Annexe V – alinéa 1 – point 2

Texte proposé par la Commission	*Amendement*
2) une description de la conception, du développement et de la fabrication du produit et des processus de gestion des vulnérabilités, et notamment:	***supprimé***
a) des informations complètes sur la conception et le développement du produit comportant des éléments numériques, y compris, le cas échéant, des dessins et des schémas et/ou une description de l'architecture du système expliquant comment les composants logiciels s'appuient les uns sur les autres ou s'alimentent et s'intègrent dans le	

traitement global;

b) des informations et des spécifications complètes concernant le processus de gestion des vulnérabilités mis en place par le fabricant, en ce compris la nomenclature des logiciels, la politique coordonnée de divulgation des vulnérabilités, la preuve de la fourniture d'une adresse de contact pour le signalement des vulnérabilités et une description des solutions techniques choisies pour la distribution sécurisée des mises à jour;

c) des informations et des spécifications complètes concernant les processus de production et de suivi du produit comportant des éléments numériques et la validation de ces processus;

Amendement 201

Proposition de règlement
Annexe V – alinéa 1 – point 3

Texte proposé par la Commission	*Amendement*
3) une ***évaluation*** des risques de cybersécurité sur la base de ***laquelle*** le produit comportant des éléments numériques est conçu, développé, produit, livré et entretenu, conformément à l'article 10 du présent règlement;	3) une ***déclaration ou un résumé*** des risques de cybersécurité sur la base ***desquels le produit comportant des éléments numériques est conçu, développé, fabriqué, livré et entretenu, conformément à l'article 10 du présent règlement et, sur requête motivée d'une autorité*** de ***surveillance du marché, pour autant que cela soit nécessaire afin que cette autorité soit en mesure de vérifier la conformité au regard des exigences essentielles énoncées à l'annexe I, une évaluation détaillée des risques de cybersécurité sur la base desquels*** le produit comportant des éléments numériques est conçu, développé, produit, livré et entretenu, conformément à l'article 10 du présent règlement;

ANNEXE: LISTE DES ENTITÉS OU PERSONNES AYANT APPORTÉ LEUR CONTRIBUTION AU RAPPORTEUR

La liste ci-après est établie, sur une base purement volontaire, sous la responsabilité exclusive du rapporteur. Le rapporteur a reçu des contributions des entités ou personnes suivantes pour l'élaboration du projet d'avis:

Entité et/ou personne
Apple
BDI Federation of German Industries
BEUC
BSA The Software Alliance
Confederation of Danish Industries
Digital Europe
ETNO
Kaspersky
Microsoft
Samsung
TIC Council
Xiaomi

PROCÉDURE DE LA COMMISSION SAISIE POUR AVIS

Titre	Exigences horizontales de cybersécurité pour les produits comportant des éléments numériques et modification du règlement (UE) 2019/1020
Références	COM(2022)0454 – C9-0308/2022 – 2022/0272(COD)
Commission compétente au fond Date de l'annonce en séance	ITRE 9.11.2022
Avis émis par Date de l'annonce en séance	IMCO 9.11.2022
Commissions associées - date de l'annonce en séance	20.4.2023
Rapporteur(e) pour avis Date de la nomination	Morten Løkkegaard 16.12.2022
Examen en commission	2.3.2023 25.4.2023 23.5.2023
Date de l'adoption	29.6.2023
Résultat du vote final	+: 41 –: 1 0: 0
Membres présents au moment du vote final	Alex Agius Saliba, Andrus Ansip, Pablo Arias Echeverría, Alessandra Basso, Biljana Borzan, Vlad-Marius Botoş, Anna Cavazzini, Dita Charanzová, Deirdre Clune, David Cormand, Alexandra Geese, Maria Grapini, Svenja Hahn, Krzysztof Hetman, Virginie Joron, Eugen Jurzyca, Arba Kokalari, Kateřina Konečná, Andrey Kovatchev, Maria-Manuel Leitão-Marques, Antonius Manders, Beata Mazurek, Leszek Miller, Anne-Sophie Pelletier, Miroslav Radačovský, René Repasi, Christel Schaldemose, Andreas Schwab, Tomislav Sokol, Ivan Štefanec, Kim Van Sparrentak, Marion Walsmann
Suppléants présents au moment du vote final	Marco Campomenosi, Maria da Graça Carvalho, Geoffroy Didier, Francisco Guerreiro, Tsvetelina Penkova, Catharina Rinzema, Kosma Złotowski
Suppléants (art. 209, par. 7) présents au moment du vote final	Asger Christensen, Nicolás González Casares, Grzegorz Tobiszowski

VOTE FINAL PAR APPEL NOMINAL
EN COMMISSION SAISIE POUR AVIS

41	+
ECR	Beata Mazurek, Grzegorz Tobiszowski, Kosma Złotowski
ID	Alessandra Basso, Marco Campomenosi, Virginie Joron
NI	Miroslav Radačovský
PPE	Pablo Arias Echeverría, Maria da Graça Carvalho, Deirdre Clune, Geoffroy Didier, Krzysztof Hetman, Arba Kokalari, Andrey Kovatchev, Antonius Manders, Andreas Schwab, Tomislav Sokol, Ivan Štefanec, Marion Walsmann
Renew	Andrus Ansip, Vlad-Marius Botoş, Dita Charanzová, Asger Christensen, Svenja Hahn, Catharina Rinzema
S&D	Alex Agius Saliba, Biljana Borzan, Nicolás González Casares, Maria Grapini, Maria-Manuel Leitão-Marques, Leszek Miller, Tsvetelina Penkova, René Repasi, Christel Schaldemose
The Left	Kateřina Konečná, Anne-Sophie Pelletier
Verts/ALE	Anna Cavazzini, David Cormand, Alexandra Geese, Francisco Guerreiro, Kim Van Sparrentak

1	-
ECR	Eugen Jurzyca

0	0

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