Procedure file

Informations de base

COD - Procédure législative ordinaire (ex-procedure codécision) Règlement	2022/0272(COD)	En attente de la position du Conseil en 1ère lecture

Acte législatif sur la cyber-résilience

Modification Règlement 2019/1020 2017/0353(COD)

Sujet
2.10.03 Normalisation, norme et marque CE/UE, certification, conformité
3.30.06 Technologies de l'information et de la communication, technologies numériques
3.30.07 Cybersécurité, politique cyberespace
3.30.25 Réseaux mondiaux et société de l'information, internet
4.60.08 Sécurité des produits et des services, responsabilité du fait du produit
6.20.02 Contrôle des exportations/importations, défense commerciale, obstacles au commerce

Priorités législatives
Déclaration commune 2022
Déclaration commune 2023-24

Acteurs principaux

Parlement européen	Commission au fond	Rapporteur(e)	Date de nomination
	ITRE Industrie, recherche et énergie		26/10/2022
		renew europe. DANTI Nicola	
		Rapporteur(e) fictif/fictive	
		epp VIRKKUNEN Henna	
		S&D COVASSI Beatrice	
		CORRAO Ignazio	
		GAZZINI Matteo	
		ECR TOŠENOVSKÝ Evžen	
		BOTENGA Marc	
	Commission pour avis	Rapporteur(e) pour avis	Date de nomination
	IMCO Marché intérieur et protection des consommateurs (Commission associée)	renew europe. LØKKEGAARD Morten	16/12/2022
	LIBE Libertés civiles, justice et affaires intérieures (Commission associée)	La commission a décidé de ne pas donner d'avis.	

Conseil de l'Union européenne		
Commission européenne	DG de la Commission	Commissaire
	Réseaux de communication, contenu et technologies	BRETON Thierry
Comité économique et social européen		

Evénements clés

15/09/2022	Publication de la proposition législative	COM(2022)0454	Résumé
09/11/2022	Annonce en plénière de la saisine de la commission, 1ère lecture		
20/04/2023	Annonce en plénière de la saisine des commissions associées		
19/07/2023	Vote en commission,1ère lecture		
19/07/2023	Décision de la commission parlementaire d'ouvrir des négociations interinstitutionnelles à travers d?un rapport adopté en commission		
27/07/2023	Dépôt du rapport de la commission, 1ère lecture	A9-0253/2023	Résumé
11/09/2023	Décision de la commission parlementaire d?engager des négociations interinstitutionnelles annoncée en plénière (Article 71)		
13/09/2023	Décision de la commission parlementaire d?engager des négociations interinstitutionnelles confirmée par la plénière (Article 71)		
23/01/2024	Approbation en commission du texte adopté en négociations interinstitutionnelles de la 1ère lecture	PE758.004 GEDA/A/(2024)000218	
11/03/2024	Débat en plénière		
12/03/2024	Décision du Parlement, 1ère lecture	T9-0130/2024	Résumé

Informations techniques

Référence de procédure	2022/0272(COD)
Type de procédure	COD - Procédure législative ordinaire (ex-procedure codécision)
Sous-type de procédure	Législation
Instrument législatif	Règlement
	Modification Règlement 2019/1020 2017/0353(COD)
Base juridique	Règlement du Parlement EP 57; Traité sur le fonctionnement de l'UE TFEU 114
Autre base juridique	Règlement du Parlement EP 159
Consultation obligatoire d'autres institutions	Comité économique et social européen
Etape de la procédure	En attente de la position du Conseil en 1ère lecture

Dossier de la commission parlementaire	ITRE/9/10122

Portail de documentation

Document de base législatif		COM(2022)0454	15/09/2022	EC	Résumé
Document annexé à la procédure		SEC(2022)0321	15/09/2022	EC	
Document annexé à la procédure		SWD(2022)0282	15/09/2022	EC	
Document annexé à la procédure		SWD(2022)0283	15/09/2022	EC	
Document annexé à la procédure		N9-0088/2022 JO C 452 29.11.2022, p. 0023	09/11/2022	EDPS	
Comité économique et social: avis, rapport		CES4103/2022	14/12/2022	ESC	
Projet de rapport de la commission		PE745.538	31/03/2023	EP	
Amendements déposés en commission		PE746.920	03/05/2023	EP	
Amendements déposés en commission		PE746.921	03/05/2023	EP	
Avis de la commission	IMCO	PE742.490	30/06/2023	EP	
Rapport déposé de la commission, 1ère lecture/lecture unique		A9-0253/2023	27/07/2023	EP	Résumé
Lettre de Coreper confirmant l'accord interinstitutionnel		GEDA/A/(2024)000218	20/12/2023	CSL	
Texte adopté du Parlement, 1ère lecture/lecture unique		T9-0130/2024	12/03/2024	EP	Résumé

Acte législatif sur la cyber-résilience

OBJECTIF : établir des exigences horizontales en matière de cybersécurité applicables aux produits comportant des éléments numériques.

ACTE PROPOSÉ : Règlement du Parlement européen et du Conseil.

RÔLE DU PARLEMENT EUROPÉEN : le Parlement européen décide conformément à la procédure législative ordinaire et sur un pied d'égalité avec le Conseil.

CONTEXTE : les produits matériels et logiciels font de plus en plus l'objet de cyberattaques réussies, ce qui a entraîné un coût annuel mondial de la cybercriminalité estimé à 5.500 milliards d'euros en 2021. Ces produits souffrent de deux problèmes majeurs qui entraînent des coûts supplémentaires pour les utilisateurs et la société : i) un faible niveau de cybersécurité, reflété par des vulnérabilités généralisées et la fourniture insuffisante et incohérente de mises à jour de sécurité pour y remédier, et ii) une compréhension et un accès insuffisants aux informations par les utilisateurs, ce qui les empêche de choisir des produits présentant des propriétés de cybersécurité adéquates ou de les utiliser de manière sécurisée.

Dans un environnement connecté, un incident de cybersécurité sur un produit peut affecter toute une organisation ou toute une chaîne d'approvisionnement, et se propager souvent au-delà des frontières du marché intérieur en quelques minutes. Cela peut entraîner une grave perturbation des activités économiques et sociales, voire mettre des vies en danger.

Si la législation existante de l'Union s'applique à certains produits comportant des éléments numériques, il n'existe pas de cadre réglementaire horizontal de l'Union établissant des exigences complètes en matière de cybersécurité pour tous les produits comportant des éléments numériques. Il est donc nécessaire d'établir un cadre juridique uniforme pour les exigences essentielles en matière de cybersécurité pour la mise sur le marché de l'Union de produits comportant des éléments numériques.

CONTENU : la proposition de la Commission vise à introduire des exigences obligatoires en matière de cybersécurité applicables aux produits comportant des éléments numériques, sur lensemble de leur cycle de vie.

Objet

Fondée sur le nouveau cadre législatif applicable à la législation sur les produits dans lUE, la proposition établit :

- des règles relatives à la mise sur le marché de produits comportant des éléments numériques afin de garantir la cybersécurité de ces produits;

- des exigences essentielles pour la conception, le développement et la production de produits comportant des éléments numériques, et des obligations pour les opérateurs économiques concernant ces produits en matière de cybersécurité;

- des exigences essentielles relatives aux processus de gestion de la vulnérabilité mis en place par les fabricants pour garantir que les

produits comportant des éléments numériques sont conformes aux exigences de cybersécurité tout au long de leur cycle de vie, et des obligations incombant aux opérateurs économiques en ce qui concerne ces processus;

- des règles relatives à la surveillance du marché et au contrôle de lapplication des règles.

Champ d'application

Le règlement proposé sappliquerait à tous les produits qui sont connectés directement ou indirectement à un autre appareil ou réseau. Il ne s'appliquerait pas aux produits pour lesquels des exigences en matière de cybersécurité sont déjà définies dans des règles européennes existantes, tels que les dispositifs médicaux, l'aviation ou les voitures.

Objectifs

La proposition poursuit deux objectifs principaux visant à assurer le bon fonctionnement du marché intérieur :

- créer les conditions propices au développement de produits sûrs comportant des éléments numériques en veillant à ce que les produits matériels et logiciels mis sur le marché présentent moins de vulnérabilités et que les fabricants prennent la sécurité au sérieux tout au long du cycle de vie d'un produit;

- créer les conditions permettant aux utilisateurs de tenir compte de la cybersécurité lorsqu'ils choisissent et utilisent des produits comportant des éléments numériques.

Obligations pour les fabricants, importateurs et distributeurs

Des obligations seraient imposées aux opérateurs économiques, à partir des fabricants jusquaux distributeurs et aux importateurs, en ce qui concerne la mise sur le marché de produits contenant des éléments numériques, en fonction de leur rôle et de leurs responsabilités dans la chaîne d'approvisionnement.

Les exigences et obligations essentielles en matière de cybersécurité stipulent que tous les produits contenant des éléments numériques ne seront mis à disposition sur le marché que si, lorsquils sont fournis de manière obligatoire, correctement installés, entretenus et utilisés aux fins auxquelles ils sont destinés ou dans des conditions raisonnablement prévisibles, ils satisfont aux exigences essentielles en matière de cybersécurité énoncées dans le règlement.

Les exigences et obligations essentielles obligeraient les fabricants à i) tenir compte de la cybersécurité dans la conception, le développement et la production des produits comportant des éléments numériques, ii) faire preuve de diligence raisonnable en ce qui concerne les aspects de sécurité lors de la conception et du développement de leurs produits, iii) faire preuve de transparence en ce qui concerne les aspects de cybersécurité qui doivent être portés à la connaissance des clients, iv) assurer un support de sécurité (mises à jour de sécurité) de manière proportionnée et v) se conformer aux exigences en matière de traitement des vulnérabilités.

Notification des organismes d'évaluation de la conformité

Le bon fonctionnement des organismes notifiés est crucial pour assurer un niveau élevé de cybersécurité et pour la confiance de toutes les parties intéressées. C'est pourquoi la proposition définit des exigences pour les autorités nationales responsables des organismes d'évaluation de la conformité (organismes notifiés). Les États membres désigneraient une autorité notifiante qui serait chargée de mettre en place et d'appliquer les procédures nécessaires à l'évaluation et à la notification des organismes d'évaluation de la conformité et au contrôle des organismes notifiés.

Processus dévaluation de la conformité

Les fabricants devraient se soumettre à un processus dévaluation de la conformité pour démontrer si les exigences spécifiées relatives à un produit ont été respectées. Lorsque la conformité du produit aux exigences applicables a été démontrée, les fabricants et les développeurs établiraient une déclaration UE de conformité et pourraient apposer le marquage CE.

Surveillance du marché

Les États membres devraient désigner des autorités de surveillance du marché, qui seraient chargées de faire respecter les obligations de la loi sur la cyberrésilience.

En cas de non-conformité, les autorités de surveillance du marché pourraient exiger des opérateurs quils mettent fin à la non-conformité et éliminent le risque, quils interdisent ou restreignent la mise à disposition dun produit sur le marché ou quils ordonnent que le produit soit retiré ou rappelé. Chacune de ces autorités pourrait infliger des amendes aux entreprises qui ne respectent pas les règles.

Application

Afin de laisser aux fabricants, aux organismes notifiés et aux États membres le temps de s'adapter aux nouvelles exigences, le règlement proposé deviendra applicable 24 mois après son entrée en vigueur, à l'exception de l'obligation de déclaration des fabricants, qui s'appliquerait à partir de 12 mois après la date d'entrée en vigueur.

Acte législatif sur la cyber-résilience

La commission de l'industrie, de la recherche et de l'énergie a adopté le rapport de Nicola DANTI (Renew, IT) sur la proposition de règlement du Parlement européen et du Conseil concernant les exigences horizontales en matière de cybersécurité applicables aux produits comportant des éléments numériques et modifiant le règlement (UE) 2019/1020.

La commission compétente a recommandé que la position du Parlement européen adoptée en première lecture dans le cadre de la procédure législative ordinaire modifie la proposition comme suit:

Mises à jour de sécurité

Le texte modifié indique que les fabricants doivent veiller, lorsque cela est techniquement possible, à ce que les produits comportant des éléments numériques fassent clairement la distinction entre les mises à jour de sécurité et les mises à jour de fonctionnalité. Les mises à jour

de sécurité, destinées à réduire le niveau de risque ou à remédier à des vulnérabilités potentielles, devraient être installées automatiquement, en particulier dans le cas des produits de consommation.

Renforcer les compétences dans un environnement numérique résistant à la cybercriminalité

Les députés ont souligné l'importance des compétences professionnelles dans le domaine de la cybersécurité, en proposant des programmes d'éducation et de formation, des initiatives de collaboration et des stratégies visant à améliorer la mobilité de la main-d'uvre.

Point de contact unique pour les utilisateurs

Afin de faciliter l'établissement de rapports sur la sécurité des produits, les fabricants devraient désigner un point de contact unique pour permettre aux utilisateurs de communiquer directement et rapidement avec eux, le cas échéant par voie électronique et d'une manière conviviale, y compris en permettant aux utilisateurs du produit de choisir le moyen de communication, qui ne devrait pas reposer uniquement sur des outils automatisés.

Les fabricants devraient rendre publiques les informations nécessaires aux utilisateurs finaux pour leur permettre d'identifier facilement leurs points de contact uniques et de communiquer avec eux.

Lignes directrices

Le texte modifié comprend des dispositions permettant à la Commission de publier des lignes directrices afin d'assurer la clarté, la certitude et la cohérence des pratiques des opérateurs économiques. La Commission devrait se concentrer sur la manière de faciliter la mise en conformité des microentreprises, des petites entreprises et des moyennes entreprises.

Procédures d'évaluation de la conformité des produits comportant des éléments numériques

Des normes harmonisées, des spécifications communes ou des systèmes européens de certification en matière de cybersécurité devraient être en place pendant six mois avant que la procédure d'évaluation de la conformité ne s'applique.

Accords de reconnaissance mutuelle (ARM)

Afin de promouvoir le commerce international, la Commission devrait s'efforcer de conclure des accords de reconnaissance mutuelle (ARM) avec les pays tiers. L'Union ne devrait établir des ARM qu'avec les pays tiers qui se trouvent à un niveau comparable de développement technique et qui ont une approche compatible en matière d'évaluation de la conformité. Les ARM devraient garantir le même niveau de protection que celui prévu par le présent règlement.

Procédure au niveau de l'UE concernant les produits comportant des éléments numériques présentant un risque important pour la cybersécurité

Lorsque la Commission a des raisons suffisantes de considérer qu'un produit comportant des éléments numériques présente un risque significatif pour la cybersécurité à la lumière de facteurs de risque non techniques, les députés ont estimé qu'elle devrait en informer les autorités de surveillance du marché concernées et adresser des recommandations ciblées aux opérateurs économiques afin de garantir la mise en place de mesures correctives appropriées.

Recettes générées par les sanctions

Les recettes générées par le paiement des sanctions devraient être utilisées pour renforcer le niveau de cybersécurité dans l'Union, notamment en développant les capacités et les compétences liées à la cybersécurité, en améliorant la cyber-résilience des opérateurs économiques, en particulier des micro-entreprises et des petites et moyennes entreprises, et plus généralement en sensibilisant le public aux questions de cybersécurité.

Évaluation et révision

Chaque année, lors de la présentation du projet de budget pour l'année suivante, la Commission devra soumettre une évaluation détaillée des tâches de l'ENISA en vertu du présent règlement telles que définies dans l'annexe VI bis et dans dautres dispositions pertinentes du droit de lUnion et devra détailler les ressources financières et humaines nécessaires pour accomplir ces tâches.

Acte législatif sur la cyber-résilience

Le Parlement européen a adopté par 517 voix pour, 12 contre et 78 abstentions, une résolution législative 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.

Le règlement sappliquera aux produits comportant des éléments numériques mis à disposition sur le marché dont lutilisation prévue ou raisonnablement prévisible comprend une connexion directe ou indirecte, logique ou physique, à un dispositif ou à un réseau.

La position du Parlement européen arrêtée en première lecture dans le cadre de la procédure législative ordinaire modifie la proposition comme suit:

Produits importants comportant des éléments numériques (annexe III)

Les produits de consommation qui sont catégorisés, en vertu du règlement, comme des produits importants comportant des éléments numériques devront faire lobjet dune procédure plus stricte dévaluation de la conformité par un organisme notifié. Sont concernés les produits domestiques intelligents comportant des fonctionnalités de sécurité, tels que i) les systèmes de gestion des identités et logiciels et dispositifs de gestion des accès privilégiés, dont lecteurs dauthentification et de contrôle daccès et lecteurs biométriques; ii) les assistants virtuels polyvalents pour maison intelligente; iii) les produits domestiques intelligents dotés de fonctionnalités de sécurité, notamment serrures, caméras de sécurité, systèmes de surveillance pour bébé et systèmes dalarme, iv) les jouets connectés ou v) les dispositifs portables personnels de santé.

La Commission pourra adopter des actes délégués pour modifier lannexe III du règlement en ajoutant une nouvelle catégorie dans chaque classe de la liste des catégories de produits comportant des éléments numériques et en précisant la définition de celle-ci, en déplaçant une

catégorie de produits dune classe à lautre ou en retirant une catégorie existante de cette liste.

Produits critiques comportant des éléments numériques (annexe IV)

Les catégories de produits critiques comportant des éléments numériques énoncées dans le règlement ont une fonctionnalité liée à la cybersécurité et remplissent une fonction qui comporte un risque important deffets néfastes du fait de sa capacité à perturber ou endommager un grand nombre dautres produits avec éléments numériques par le biais dune manipulation directe.

La Commission pourra adopter des actes délégués afin de déterminer quels produits comportant des éléments numériques dont la fonctionnalité de base est celle dune catégorie de produits qui figure à lannexe IV du règlement doivent être tenus dobtenir un certificat de cybersécurité européen au minimum au niveau dassurance dit «substantiel» dans le cadre dun schéma européen de certification de cybersécurité, afin de démontrer leur conformité aux exigences essentielles énoncées dans le règlement, à condition quun schéma européen de certification de cybersécurité couvrant ces catégories de produits ait été adopté et soit à la disposition des fabricants.

Consultation des parties intéressées

Lors de lélaboration des mesures de mise en uvre du règlement, la Commission devra consulter les parties intéressées, telles que les autorités des États membres concernées, les entreprises du secteur privé, y compris les microentreprises et les petites et moyennes entreprises, la communauté des logiciels ouverts, les associations de consommateurs, le milieu universitaire et les organismes et organes compétents de lUnion, ainsi que les groupes dexperts établis au niveau de lUnion.

Afin de répondre aux besoins des professionnels, les États membres, avec, le cas échéant, le soutien de la Commission, du Centre européen de compétences en matière de cybersécurité et de lAgence de l'Union européenne pour la cybersécurité (ENISA), devront favoriser des mesures et des stratégies visant à développer des compétences en matière de cybersécurité et à créer des outils organisationnels et technologiques pour garantir une disponibilité suffisante de professionnels qualifiés afin de soutenir les activités des autorités de surveillance du marché et des organismes dévaluation de la conformité.

Obligation des fabricants

Le fabricant devra procéder à une évaluation des risques de cybersécurité associés à un produit comportant des éléments numériques. Lévaluation des risques de cybersécurité doit être documentée et mise à jour selon les besoins au cours dune période dassistance. Lorsquil met sur le marché un produit comportant des éléments numériques, et pendant la période dassistance, le fabricant devra veiller à ce que les vulnérabilités de ce produit, y compris de ses composants, soient gérées efficacement et conformément aux exigences essentielles. Lorsquil identifie une vulnérabilité dans un composant, y compris un composant logiciel ouvert, qui est intégré au produit comportant des éléments numériques, le fabricant devra signaler la vulnérabilité à la personne ou à lentité qui assure la maintenance du composant, et sattaquer et remédier à la vulnérabilité.

Le fabricant devra :

- fixer la période dassistance de sorte quelle reflète la durée pendant laquelle le produit est censé pouvoir être utilisé, en tenant compte, en particulier, des attentes raisonnables des utilisateurs, de la nature du produit, y compris de son utilisation prévue, ainsi que du droit de lUnion applicable déterminant la durée de vie des produits comportant des éléments numériques;

- veiller à ce que chaque mise à jour de sécurité qui a été mise à la disposition des utilisateurs au cours de la période dassistance, reste disponible après son émission pendant au moins 10 ans après la mise sur le marché du produit comportant des éléments numériques ou pendant le reste de la période dassistance;

- désigner un point de contact unique pour permettre aux utilisateurs de communiquer directement et rapidement avec lui, notamment afin de faciliter le signalement des vulnérabilités du produit comportant des éléments numériques.

Obligations en matière de communication dinformations incombant aux fabricants

Un fabricant devra notifier toute vulnérabilité activement exploitée contenue dans le produit comportant des éléments numériques dont il prend connaissance simultanément au centre de réponse aux incidents de sécurité informatique (CSIRT) désigné comme coordinateur et à lENISA. Le fabricant devra soumettre i) une alerte précoce de vulnérabilité activement exploitée, au plus tard 24 heures après en avoir eu connaissance, ii) une notification de vulnérabilité au plus tard 72 heures après avoir eu connaissance de la vulnérabilité activement exploitée. Un fabricant devra également notifier tout incident grave ayant un impact sur la sécurité du produit comportant des éléments numériques.

Le fabricant mais aussi dautres personnes physiques ou morales pourront notifier toute vulnérabilité contenue dans un produit comportant des éléments numériques ainsi que les cybermenaces susceptibles daffecter le profil de risque dun produit comportant des éléments numériques, de manière volontaire. Afin de simplifier les obligations de signalement des fabricants, lENISA mettra en place une plateforme unique de notification.

Transparence

KOLAJA Marcel	Rapporteur(e) fictif/fictive pour avis	IMCO	30/11/2023	Eclipse Foundation AISBL Linux Foundation Europe Red Hat Limited the Mozilla Foundation
KOLAJA Marcel	Rapporteur(e) fictif/fictive pour avis	IMCO	16/11/2023	Red Hat Limited
DANTI Nicola	Rapporteur(e)	ITRE	16/11/2023	APCO Worldwide
DANTI Nicola	Rapporteur(e)	ITRE	10/11/2023	OpenForum Europe AISBL

DANTI Nicola	Rapporteur(e)	ITRE	09/11/2023	American Chamber of Commerce in Belgium CNH Industrial ChargePoint Network (Netherlands) BV IBM Corporation Microsoft Corporation Oracle Workday
COVASSI Beatrice	Rapporteur(e) fictif/fictive	ITRE	06/11/2023	Apple Inc.
DANTI Nicola	Rapporteur(e)	ITRE	03/11/2023	DIGITALEUROPE Samsung Electronics Europe Schneider Electric Siemens AG
DANTI Nicola	Rapporteur(e)	ITRE	03/11/2023	GitHub, Inc.
DANTI Nicola	Rapporteur(e)	ITRE	26/10/2023	NLnet Labs
COVASSI Beatrice	Rapporteur(e) fictif/fictive	ITRE	25/10/2023	European Internet Forum
MELCHIOR Karen	Membre	20/02/2024	Match Group	
MELCHIOR Karen	Membre	15/02/2024	Apple Inc.	
FUGLSANG Niels	Membre	22/06/2023	Confederation of Danish Industry	
REPASI René	Membre	26/04/2023	Verbraucherzentrale Bundesverband	
KALJURAND Marina	Membre	09/02/2023	Cybersecurity Coalition	