Procedure file

Informations de base

COD - Procédure législative ordinaire (ex-procedure codécision) Règlement	2017/0225(COD)	Procédure terminée
Agence de cybersécurité de l'UE (ENISA) et certification de cybersécurité des TIC ("Cybersecurity Act") Abrogation Règlement (EU) 526/2013 2010/0275(COD) Sujet 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 8.40.08 Agences et organes de l'Union		

Acteurs principaux

Parlement européen

Commission au fond	Rapporteur(e)	Date de nomination
ITRE Industrie, recherche et énergie	NIEBLER Angelika Rapporteur(e) fictif/fictive KOUROUMBASHEV Peter TOŠENOVSKÝ Evžen TELIČKA Pavel DALUNDE Jakop G. TAMBURRANO Dario LETARD-LECHEVALIER Christelle	27/10/2017

Commission pour avis	Rapporteur(e) pour avis	Date de nomination
AFET Affaires étrangères	La commission a décidé de ne pas donner d'avis.	
BUDG Budgets	GEIER Jens	26/09/2017
IMCO Marché intérieur et protection des consommateurs (Commission associée)		25/09/2017

		S&D DANTI Nicola	
	LIBE Libertés civiles, justice et affaires intérieures		11/03/2019
		FRANZ Romeo	
Conseil de l'Union européenne	Formation du Conseil	Réunion	Date
	Affaires générales	3685	09/04/2019
	Affaires générales	3578	20/11/2017
Commission européenne	DG de la Commission	Commissaire	
	Réseaux de communication, contenu et technologies	KING Julian	
Comité économique et social européen			
Comité européen des régions			

Evénements clés

13/09/2017	Publication de la proposition législative	COM(2017)0477	Résumé
23/10/2017	Annonce en plénière de la saisine de la commission, 1ère lecture		
20/11/2017	Adoption de résolution/conclusions par le Conseil		
18/01/2018	Annonce en plénière de la saisine des commissions associées		
10/07/2018	Vote en commission,1ère lecture		
10/07/2018	Décision de la commission parlementaire d'ouvrir des négociations interinstitutionnelles à travers d?un rapport adopté en commission		
30/07/2018	Dépôt du rapport de la commission, 1ère lecture	A8-0264/2018	
10/09/2018	Décision de la commission parlementaire d?engager des négociations interinstitutionnelles annoncée en plénière (Article 71)		
12/09/2018	Décision de la commission parlementaire d?engager des négociations interinstitutionnelles confirmée par la plénière (Article 71)		
14/01/2019	Approbation en commission du texte adopté en négociations interinstitutionnelles de la 1ère lecture		
11/03/2019	Débat en plénière		
12/03/2019	Résultat du vote au parlement		
12/03/2019	Décision du Parlement, 1ère lecture	T8-0151/2019	Résumé
09/04/2019	Adoption de l'acte par le Conseil après la 1ère lecture du Parlement		

17/04/2019	Signature de l'acte final		
17/04/2019	Fin de la procédure au Parlement		
07/06/2019	Publication de l'acte final au Journal officiel		

Informations techniques

Référence de procédure	2017/0225(COD)
Type de procédure	COD - Procédure législative ordinaire (ex-procedure codécision)
Sous-type de procédure	Législation
Instrument législatif	Règlement
	Abrogation Règlement (EU) 526/2013 2010/0275(COD)
Base juridique	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 Comité européen des régions
Etape de la procédure	Procédure terminée
Dossier de la commission parlementaire	ITRE/8/11042

Portail de documentation

Document de base législatif		COM(2017)0477	13/09/2017	EC	Résumé
Document annexé à la procédure		SWD(2017)0500	13/09/2017	EC	
Document annexé à la procédure		SWD(2017)0501	13/09/2017	EC	
Document annexé à la procédure		SWD(2017)0502	13/09/2017	EC	
Comité économique et social: avis, rapport		CES4390/2017	14/02/2018	ESC	
Avis de la commission	LIBE	PE615.394	16/03/2018	EP	
Projet de rapport de la commission		PE619.373	27/03/2018	EP	
Avis de la commission	BUDG	PE619.094	23/04/2018	EP	
Amendements déposés en commission		PE621.015	30/04/2018	EP	
Amendements déposés en commission		PE621.098	30/04/2018	EP	
Avis de la commission	IMCO	PE616.831	22/05/2018	EP	
Rapport déposé de la commission, 1ère lecture/lecture unique		A8-0264/2018	30/07/2018	EP	
Texte adopté du Parlement, 1ère lecture/lecture unique		T8-0151/2019	12/03/2019	EP	Résumé
Projet d'acte final		00086/2018/LEX	17/04/2019	CSL	
Réaction de la Commission sur le texte adopté en plénière		SP(2019)393	30/04/2019	EC	

Acte final

Règlement 2019/881

JO L 151 07.06.2019, p. 0015 Résumé

Agence de cybersécurité de l'UE (ENISA) et certification de cybersécurité des TIC ("Cybersecurity Act")

OBJECTIF: réformer l'actuelle Agence européenne pour la sécurité des réseaux et de l'information (ENISA) en vue de doter l'UE d'une capacité accrue en matière de cybersécurité et définir un cadre pour la mise en place dun système européen de certification en matière cybersécurité.

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: l'Union européenne a déjà pris un certain nombre de mesures pour accroître la résilience face aux cyberattaques. Depuis la première stratégie européenne de cybersécurité adoptée en 2013, des développements importants ont eu lieu, y compris le deuxième mandat de l'Agence européenne pour la sécurité des réseaux et de l'information (ENISA) et l'adoption de la directive sur la sécurité des réseaux et des systèmes d'information (Directive SRI) qui constituent la base de la présente proposition.

En 2016, la Commission européenne a adopté une communication sur le renforcement du système européen de cyber-résilience, dans laquelle d'autres mesures ont été annoncées pour mieux protéger l'UE.

Le Conseil a rappelé que le règlement (UE) n° 526/2013 sur lENISA était l'un des éléments essentiels d'un cadre de résilience informatique de l'UE et a demandé à la Commission de prendre d'autres mesures pour aborder la question de la certification au niveau européen. En 2017, il sest félicité de l'intention de la Commission d'examiner la stratégie de la cybersécurité en septembre et de proposer d'autres actions ciblées avant la fin de 2017.

ANALYSE D'IMPACT: l'analyse d'impact a identifié plusieurs problèmes tels que: la fragmentation des politiques et des approches de la cybersécurité dans les États membres; des ressources dispersées et des approches disparates au sein des institutions, organismes et organes de l'UE; une sensibilisation et une information insuffisantes des citoyens et des entreprises, conjuguée à l'émergence croissante de multiples systèmes nationaux et sectoriels de certification.

L'analyse a permis de conclure qu'une ENISA réformée combinée à un cadre général de certification de la cybersécurité de l'UE en matière de technologies de linformation des communications (TIC) était l'option privilégiée.

CONTENU: la proposition vise à réviser le mandat actuel de l'ENISA et à définir un ensemble renouvelé de tâches et de fonctions, en vue de soutenir efficacement les États membres, les institutions de l'UE et les efforts des autres parties prenantes dans lobjectif dassurer un cyberespace sécurisé dans l'Union européenne.

Le nouveau mandat proposé vise à donner à l'Agence un rôle plus important et plus central, notamment en contribuant à la mise en uvre de la directive SRI, et en devenant un centre d'expertise pour aider les États membres et la Commission à créer et à appliquer le cadre de certification à l'échelle de l'UE.

En particulier, la proposition vise à:

- transformer l'actuelle Agence européenne pour la sécurité des réseaux et de l'information (ENISA) en une Agence européenne de la cybersécurité, qui améliorera la coordination et la coopération entre les États membres et les institutions, organismes et organes de l'UE;
- établir un cadre de certification à léchelle l'UE qui assurera la fiabilité de milliards de dispositifs («Internet des objets») qui pilotent dorénavant les infrastructures critiques, telles que les réseaux d'énergie et de transport, mais aussi de nouveaux équipements grand public, tels que les voitures connectées.

Une Agence européenne pour la cybersécurité: l'Agence disposerait d'un mandat permanent pour aider les États membres à prévenir efficacement les cyberattaques et à y répondre.

En vue daméliorer la préparation de l'UE en cas d'attaques, elle organiserait chaque année des exercices de cybersécurité paneuropéens et assurerait un meilleur partage des connaissances et des informations sur les menaces par la création de centres de partage et d'analyse de linformation.

Elle contribuerait aussi à la mise en uvre de la directive SRI, qui impose des obligations de signalement des incidents graves aux autorités nationales.

LAgence aiderait en outre à créer et à appliquer le cadre de certification à l'échelle de l'UE proposé par la Commission pour garantir que les produits et les services répondent à toutes les exigences de cybersécurité applicables.

La proposition comprend également les dispositions visant à faciliter la lutte contre la fraude, la corruption et d'autres activités illégales, ainsi que des dispositions en matière de dotation en personnel et de budget.

Un cadre de certification de la cybersécurité de l'UE: actuellement, il existe différents systèmes de certification de sécurité pour les produits TIC dans l'UE. L'Agence mettra en place un processus de certification. Le cadre de certification proposé à l'échelle de l'UE crée un ensemble complet de règles, d'exigences techniques, de normes et de procédures destiné à convenir à chaque système. Chaque système de certification serait basé sur un accord au niveau de l'UE pour l'évaluation des propriétés de sécurité d'un produit TIC spécifique (par exemple : carte à puce).

La proposition établit les principaux effets juridiques des systèmes européens de certification de la cybersécurité, à savoir: i) l'obligation de mettre en uvre le régime au niveau national et le caractère volontaire de la certification; ii) l'effet invalidant des systèmes de certification de la

cybersécurité européenne sur les régimes nationaux pour les mêmes produits ou services. Elle définit également la procédure d'adoption des systèmes européens de certification ainsi que les rôles respectifs de la Commission, de l'Agence et du Groupe européen de certification de la cybersécurité.

INCIDENCE BUDGÉTAIRE: le total des crédits, y compris les dépenses administratives, de 2019 à 2022 est estimé à 86,038 millions d'EUR.

Agence de cybersécurité de l'UE (ENISA) et certification de cybersécurité des TIC ("Cybersecurity Act")

Le Parlement européen a adopté par 586 voix pour, 44 contre et 36 abstentions, une résolution législative sur la proposition de règlement du Parlement européen et du Conseil relatif à lENISA, Agence de lUnion européenne pour la cybersécurité, et abrogeant le règlement (UE) nº 526/2013, et relatif à la certification des technologies de linformation et des communications en matière de cybersécurité (règlement sur la cybersécurité).

La position du Parlement européen arrêtée en première lecture suivant la procédure législative ordinaire a modifié la proposition de la Commission comme suit :

Pouvoirs renforcés pour lAgence de lUE pour la cybersécurité (ENISA)

En vue d'assurer le bon fonctionnement du marché intérieur tout en cherchant à atteindre un niveau élevé de cybersécurité, le règlement proposé fixerait les objectifs, les tâches et les questions organisationnelles concernant l'ENISA (l'Agence de l'Union européenne pour la cybersécurité).

LENISA exécuterait ses tâches dans le but de parvenir à un niveau commun élevé de cybersécurité dans l'ensemble de l'Union, y compris en aidant activement les États membres et les institutions, organes et organismes de l'Union à améliorer la cybersécurité. Elle servirait de point de référence pour les conseils et compétences en matière de cybersécurité pour les institutions, organes et organismes de l'Union ainsi que pour les autres parties prenantes concernées de l'Union. À cette fin, elle devrait développer ses ressources propres, y compris ses capacités et aptitudes techniques.

LENISA devrait, entre autres :

- assister les États membres et les institutions, organes et organismes de l'Union i) à mettre en place les capacités et la préparation requises pour prévenir et détecter les cybermenaces et incidents et y réagir ; ii) à élaborer et à promouvoir des politiques en matière de cybersécurité visant à soutenir la disponibilité ou l'intégrité générales du noyau public de l'internet ouvert; iii) à mettre en uvre, sur une base volontaire, des politiques en matière de divulgation des vulnérabilités;
- favoriser le partage d'informations et la coordination au niveau de l'Union, entre les États membres, les institutions, organes et organismes de l'Union et les parties prenantes concernées des secteurs public et privé en ce qui concerne les questions liées à la cybersécurité ;
- favoriser le recours à la certification européenne de cybersécurité en vue d'éviter la fragmentation du marché intérieur ;
- soutenir les États membres dans le domaine de la sensibilisation et de l'éducation à la cybersécurité en favorisant une coordination plus étroite et l'échange de bonnes pratiques entre les États membres. Un tel soutien pourrait consister à développer un réseau de points de contact nationaux en matière d'éducation ainsi quune plateforme de formation à la cybersécurité ;
- sensibiliser le public aux risques liés à la cybersécurité et fournir, à l'intention des citoyens, des organisations et des entreprises, des orientations sur les bonnes pratiques à adopter par les utilisateurs individuels, y compris en matière d'hygiène informatique et d'habileté numérique;
- faciliter la gestion technique des incidents ayant un impact significatif ou substantiel, en particulier en soutenant le partage volontaire de solutions techniques entre États membres ou en produisant des informations techniques combinées, telles que des solutions techniques partagées volontairement par les États membres ;
- promouvoir les concepts de sécurité dès la conception et de protection de la vie privée dès la conception au niveau de l'Union ;
- contribuer, s'il y a lieu, à une coopération avec des organisations telles que l'OCDE, l'OSCE et l'OTAN par exemple au moyen dexercices conjoints dans le domaine de la cybersécurité.

LENISA devrait tenir le Parlement européen régulièrement informé de ses activités.

Réseau des agents de liaison nationaux

Le conseil d'administration devrait créer, sur proposition du directeur exécutif, un réseau des agents de liaison nationaux composé de représentants de tous les États membres (les agents de liaison nationaux). Ce réseau faciliterait l'échange d'informations entre l'ENISA et les États membres et aiderait l'ENISA à faire connaître ses activités et à diffuser les résultats de ses travaux et ses recommandations auprès des parties prenantes concernées dans l'ensemble de l'Union.

Cadre européen de certification de cybersécurité

Le texte amendé crée le premier dispositif européen de certification en matière de cybersécurité afin de garantir que les produits, les processus et les services vendus dans les pays de lUE soient conformes aux normes de cybersécurité.

La Commission devrait publier, au plus tard un an après l'entrée en vigueur du règlement, un programme de travail glissant de l'Union pour la certification européenne de cybersécurité qui recense les priorités stratégiques pour les futurs schémas européens de certification de cybersécurité. Elle devrait tenir à jour un site internet dédié fournissant des informations sur les schémas européens de certification de cybersécurité, les certificats de cybersécurité européens et les déclarations de conformité de l'UE.

Dans un souci d'équivalence des normes, dans l'ensemble de l'Union, en ce qui concerne les certificats de cybersécurité européens et les déclarations de conformité de l'UE, les autorités nationales de certification de cybersécurité feraient l'objet d'un examen par les pairs.

Agence de cybersécurité de l'UE (ENISA) et certification de cybersécurité des TIC ("Cybersecurity Act")

OBJECTIF : réformer l'actuelle Agence européenne pour la sécurité des réseaux et de l'information (ENISA) en vue de doter l'UE d'une capacité accrue en matière de cybersécurité et définir un cadre pour la mise en place dun système européen de certification en matière cybersécurité.
ACTE LÉGISLATIF : Règlement (UE) 2019/881 du Parlement européen et du Conseil relatif à lENISA (Agence de lUnion européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de linformation et des communications, et abrogeant le règlement (UE) n° 526/2013 (règlement sur la cybersécurité).
CONTENU : en vue dassurer le bon fonctionnement du marché intérieur tout en cherchant à atteindre un niveau élevé de cybersécurité, de cyber-résilience et de confiance au sein de lUnion, le règlement fixe:

- les objectifs, les tâches et les questions organisationnelles concernant lENISA (lAgence de lUnion européenne pour la cybersécurité); et
- un cadre pour la mise en place de schémas européens de certification de cybersécurité dans le but de garantir un niveau adéquat de cybersécurité des produits TIC, services TIC et processus TIC dans lUnion, ainsi que dans le but déviter la fragmentation du marché intérieur pour ce qui est des schémas de certification dans lUnion.

Agence de lUnion européenne pour la cybersécurité (ENISA)
Le règlement renforce l'actuelle Agence de l'Union européenne chargée de la sécurité des réseaux et de l'information (ENISA) pour en faire un organe permanent, l'Agence de l'UE pour la cybersécurité.
LENISA exécutera les tâches qui lui sont assignées par le règlement dans le but de parvenir à un niveau commun élevé de cybersécurité dans lensemble de lUnion. Elle servira de point de référence pour les conseils et compétences en matière de cybersécurité pour les institutions, organes et organismes de lUnion ainsi que pour les autres parties prenantes concernées de lUnion.
Les tâches de lENISA consisteront entre autres à :

- assister les institutions, organes et organismes de lUnion, ainsi que les États membres, dans lélaboration et la mise en uvre des politiques de lUnion liées à la cybersécurité et à les aider à accroître la protection de leurs réseaux et systèmes dinformation, à améliorer les capacités de cyber-résilience et de cyber-réaction, et à développer des aptitudes et des compétences dans le domaine de la cybersécurité ;
- soutenir la politique de l'UE en matière de certification de la cybersécurité, par exemple en jouant un rôle central dans l'élaboration des systèmes de certification ;
- promouvoir l'utilisation du nouveau système de certification, par exemple en créant un site web fournissant des informations sur les certificats ;
- favoriser la coopération, notamment le partage dinformations et la coordination au niveau de lUnion ;
- soutenir les actions des États membres pour prévenir les cybermenaces et réagir à celles-ci, notamment en cas dincidents transfrontières ;
- promouvoir un niveau élevé de sensibilisation des citoyens, des organisations et des entreprises aux questions liées à la cybersécurité, y compris en matière dhygiène informatique et dhabileté numérique ;
- organiser des exercices réguliers de cybersécurité à l'échelle de l'UE, y compris un exercice global à grande échelle une fois tous les deux ans ;
- produire des analyses stratégiques à long terme des cybermenaces et des incidents afin didentifier les tendances émergentes et contribuer à prévenir les incidents.

Le mandat prévoit aussi un réseau d'agents de liaison nationaux afin de faciliter l'échange d'informations entre l'ENISA et les États membres.
Un groupe consultatif de lENISA composé dexperts reconnus représentant les parties prenantes concernées, ainsi quun groupe des parties prenantes pour la certification de cybersécurité seront établis.
Cadre européen de certification de cybersécurité
Le règlement crée un mécanisme pour l'établissement de systèmes européens de certification de cybersécurité afin de garantir que les produits, les processus et les services TIC vendus dans les pays de lUE soient conformes aux normes de cybersécurité. Les certificats délivrés dans le cadre de ces systèmes seront valables dans tous les pays de l'UE.
La Commission devra publier un programme de travail de l'Union pour la certification européenne de cybersécurité qui recense les priorités stratégiques pour les futurs schémas européens de certification de cybersécurité. Elle devra tenir à jour un site internet dédié fournissant des informations sur les schémas

européens de certification de cybersécurité, les certificats de cybersécurité européens et les déclarations de conformité de l'UE.
Les systèmes de certification eux-mêmes s'appuieront sur ce qui existe déjà aux niveaux international, européen et national. Les systèmes seront adoptés par la Commission et mis en uvre et contrôlés par des autorités nationales de certification de cybersécurité.
La certification sera volontaire, sauf disposition contraire dans le droit de l'UE ou des États membres. La Commission surveillera régulièrement l'impact des systèmes de certification et évaluera leur niveau d'utilisation par les fabricants et les fournisseurs de services.
Il existera trois niveaux d'assurance différents, selon le niveau de risque associé à l'utilisation prévue du produit, à savoir «élémentaire», «substantiel» ou «élevé». Au niveau le plus élémentaire, les fabricants ou les fournisseurs de services pourront effectuer eux-mêmes l'évaluation de conformité.
Dans un souci déquivalence des normes, dans lensemble de lUnion, en ce qui concerne les certificats de cybersécurité européens, les autorités nationales de certification de cybersécurité feront lobjet dun examen par les pairs.
ENTRÉE EN VIGUEUR : 27.6.2019. Certaines dispositions sappliqueront à partir du 28.6.2021.