

# Procedure file

Informations de base	
COD - Procédure législative ordinaire (ex-procedure codécision) Règlement	2023/0109(COD)
En attente de la position du Conseil en 1ère lecture	
Mesures visant à renforcer la solidarité de l'Union et ses capacités de détection, de préparation et de réaction face aux menaces et aux incidents de cybersécurité	
Sujet	
3.30.06 Technologies de l'information et de la communication, technologies numériques	
3.30.07 Cybersécurité, politique cyberspace	
3.30.25 Réseaux mondiaux et société de l'information, internet	

Acteurs principaux			
Parlement européen	Commission au fond	Rapporteur(e)	Date de nomination
	<b>ITRE</b> <a href="#">Industrie, recherche et énergie</a>		02/05/2023
		 <a href="#">GÁLVEZ Lina</a>	
		Rapporteur(e) fictif/fictive	
		 <a href="#">NIEBLER Angelika</a>	
		 <a href="#">GROOTHUIS Bart</a>	
		 <a href="#">NIINISTÖ Ville</a>	
		 <a href="#">TOŠENOVSKÝ Evžen</a>	
	Commission pour avis	Rapporteur(e) pour avis	Date de nomination
	<b>AFET</b> <a href="#">Affaires étrangères</a>		16/06/2023
		 <a href="#">TUDORACHE Dragoș</a>	
	<b>BUDG</b> <a href="#">Budgets</a>	La commission a décidé de ne pas donner d'avis.	
	<b>CONT</b> <a href="#">Contrôle budgétaire</a>	La commission a décidé de ne pas donner d'avis.	
	<b>IMCO</b> <a href="#">Marché intérieur et protection des consommateurs</a>	La commission a décidé de ne pas donner d'avis.	
	<b>TRAN</b> <a href="#">Transports et tourisme</a>		07/07/2023
		 <a href="#">FALCĂ Gheorghe</a>	
	<b>LIBE</b> <a href="#">Libertés civiles, justice et affaires intérieures</a>	La commission a décidé de ne pas donner d'avis.	

Evénements clés			
18/04/2023	Publication de la proposition législative	COM(2023)0209	Résumé
01/06/2023	Annonce en plénière de la saisine de la commission, 1ère lecture		
07/12/2023	Vote en commission, 1ère lecture		
07/12/2023	Décision de la commission parlementaire d'ouvrir des négociations interinstitutionnelles à travers d'un rapport adopté en commission		
08/12/2023	Dépôt du rapport de la commission, 1ère lecture	<a href="#">A9-0426/2023</a>	Résumé
11/12/2023	Décision de la commission parlementaire d'engager des négociations interinstitutionnelles annoncée en plénière (Article 71)		
13/12/2023	Décision de la commission parlementaire d'engager des négociations interinstitutionnelles confirmée par la plénière (Article 71)		
20/03/2024	Approbation en commission du texte adopté en négociations interinstitutionnelles de la 1ère lecture	PE760.882 GEDA/A/(2024)001689	
24/04/2024	Résultat du vote au parlement		
24/04/2024	Décision du Parlement, 1ère lecture	<a href="#">T9-0355/2024</a>	Résumé

Informations techniques	
Référence de procédure	2023/0109(COD)
Type de procédure	COD - Procédure législative ordinaire (ex-procedure codécision)
Sous-type de procédure	Législation
Instrument législatif	Règlement
Base juridique	Traité sur le fonctionnement de l'UE TFEU 173-p3; Traité sur le fonctionnement de l'UE TFEU 322-p1
Consultation obligatoire d'autres institutions	<a href="#">Comité économique et social européen</a>
Etape de la procédure	En attente de la position du Conseil en 1ère lecture
Dossier de la commission parlementaire	ITRE/9/11824

Portail de documentation					
Document de base législatif		COM(2023)0209	18/04/2023	EC	Résumé

Comité économique et social: avis, rapport		<a href="#">CES2408/2023</a>	13/07/2023	ESC	
Projet de rapport de la commission		<a href="#">PE752.795</a>	04/09/2023	EP	
Amendements déposés en commission		<a href="#">PE753.628</a>	22/09/2023	EP	
Avis de la commission	TRAN	<a href="#">PE752.607</a>	25/10/2023	EP	
Avis de la commission	AFET	<a href="#">PE750.145</a>	27/10/2023	EP	
Comité des régions: avis		<a href="#">CDR2191/2023</a>	29/11/2023	CofR	
Rapport déposé de la commission, 1ère lecture/lecture unique		<a href="#">A9-0426/2023</a>	08/12/2023	EP	Résumé
Lettre de Coreper confirmant l'accord interinstitutionnel		GEDA/A/(2024)001689	21/03/2024	CSL	
Texte adopté du Parlement, 1ère lecture/lecture unique		<a href="#">T9-0355/2024</a>	24/04/2024	EP	Résumé

<b>Informations complémentaires</b>		
Document de recherche	<a href="#">Briefing</a>	27/11/2023

## Mesures visant à renforcer la solidarité de l'Union et ses capacités de détection, de préparation et de réaction face aux menaces et aux incidents de cybersécurité

**OBJECTIF** : établir des mesures visant à renforcer la solidarité et les capacités de l'Union à détecter les menaces et les incidents liés à la cybersécurité, à s'y préparer et à y répondre (loi de IUE sur la cybersolidarité).

**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'ampleur, la fréquence et l'impact des incidents de cybersécurité augmentent, y compris les attaques de la chaîne d'approvisionnement visant le cyberespionnage, les ransomwares ou les perturbations. Ils représentent une menace majeure pour le fonctionnement des réseaux et des systèmes d'information. Compte tenu de l'évolution rapide du paysage des menaces, la menace d'éventuels incidents à grande échelle causant des perturbations ou des dommages importants aux infrastructures critiques exige une préparation accrue à tous les niveaux du cadre de cybersécurité de l'Union. Cette menace va au-delà de l'agression militaire de la Russie contre l'Ukraine et devrait persister compte tenu de la multiplicité des acteurs étatiques, criminels et hacktivistes impliqués dans les tensions géopolitiques actuelles.

**CONTENU** : la proposition de loi sur la cybersolidarité vise à établir les capacités de IUE pour rendre l'Europe plus résiliente et plus réactive face aux cybermenaces, tout en renforçant le mécanisme de coopération existant. Elle contribuera à assurer un paysage numérique sûr et sécurisé pour les citoyens et les entreprises et à protéger les entités critiques et les services essentiels, tels que les hôpitaux et les services publics.

Le règlement proposé établit des mesures visant à renforcer les capacités de l'Union à détecter les menaces et les incidents liés à la cybersécurité, à s'y préparer et à y répondre, notamment par les actions suivantes:

### Bouclier européen de cybersécurité

Une infrastructure paneuropéenne interconnectée de centres d'opérations de sécurité (cyberbouclier européen) sera mise en place pour développer des capacités avancées permettant à l'Union de détecter, d'analyser et de traiter les données relatives aux menaces et incidents cybernétiques dans l'Union. Le cyberbouclier européen sera composé de centres d'opérations de sécurité (SOC) dans toute l'UE, rassemblés dans plusieurs plateformes SOC multinationales, construits avec le soutien du programme pour une Europe numérique (PED) pour compléter le financement national. Le cyberbouclier sera chargé d'améliorer la détection, l'analyse et la réponse aux cybermenaces. Ces SOC utiliseront des technologies avancées telles que l'intelligence artificielle (IA) et l'analyse de données pour détecter et partager les avertissements sur de telles menaces avec les autorités transfrontalières. Ils permettront une intervention plus rapide et plus efficace en cas de menaces majeures.

### Mécanisme de cyberurgence

Le mécanisme de cyberurgence améliorera la résilience de l'Union face aux menaces majeures en matière de cybersécurité et permettra de se préparer à l'impact à court terme d'incidents de cybersécurité importants et à grande échelle et de l'atténuer, dans un esprit de solidarité. Il prévoit des actions de soutien à la préparation, notamment des tests coordonnés d'entités opérant dans des secteurs hautement critiques (tels que la finance, l'énergie et les soins de santé), une réponse et un rétablissement immédiat en cas d'incidents de cybersécurité importants ou à grande échelle, l'atténuation des cybermenaces importantes et des actions d'assistance mutuelle.

Il est également prévu de créer une réserve européenne de cybersécurité constituée de services de réaction aux incidents fournis par des fournisseurs de confiance sélectionnés, prêts intervenir, à la demande d'un État membre ou des institutions, organes et agences de l'Union, en

cas d'incident de cybersécurité important ou de grande ampleur.

#### Mécanisme européen d'examen des incidents de cybersécurité

La proposition de règlement prévoit également la mise en place d'un mécanisme d'examen des incidents de cybersécurité, chargé d'évaluer et d'examiner les incidents de cybersécurité spécifiques. À la demande de la Commission ou des autorités nationales (le réseau EU-CyCLONE ou le réseau des CSIRT), l'Agence européenne de cybersécurité (ENISA) sera chargée de l'examen d'un incident de cybersécurité spécifique, important ou à grande échelle, et devra rédiger un rapport comprenant les enseignements tirés et, le cas échéant, des recommandations visant à améliorer la réponse de l'Union en matière de cybersécurité.

#### Implications budgétaires

Le bouclier de cybersécurité de l'UE et le mécanisme d'urgence en matière de cybersécurité du présent règlement bénéficieront d'un financement au titre de l'objectif stratégique «Cybersécurité» du programme pour une Europe numérique (PED).

Le budget total comprend une augmentation de 100 millions d'euros que le présent règlement propose de réaffecter à partir d'autres objectifs stratégiques du programme. Cela portera le nouveau montant total disponible pour les actions de cybersécurité dans le cadre du PED à 842,8 millions d'euros. Une partie des 100 millions d'euros supplémentaires renforcera le budget géré par les CETC pour mettre en œuvre des actions sur les SOC et la préparation dans le cadre de leur(s) programme(s) de travail. En outre, le financement supplémentaire servira à soutenir la mise en place de la réserve de cybersécurité de l'UE.

Il complète le budget déjà prévu pour des actions similaires dans le programme de travail principal du PED et du groupe de travail sur la cybersécurité pour la période 2023-2027, ce qui pourrait porter le total à 551 millions d'euros pour 2023-2027, alors que 115 millions d'euros ont déjà été consacrés sous forme de projets pilotes pour 2021-2022. En incluant les contributions des États membres, le budget global pourrait s'élever à 1,109 milliard d'euros.

## Mesures visant à renforcer la solidarité de l'Union et ses capacités de détection, de préparation et de réaction face aux menaces et aux incidents de cybersécurité

---

La commission de l'industrie, de la recherche et de l'énergie a adopté le rapport de Lina GÁLVEZ MUÑOZ (S&D, ES) sur la proposition de règlement du Parlement européen et du Conseil établissant des mesures destinées à renforcer la solidarité et les capacités dans l'Union afin de détecter les menaces et incidents de cybersécurité, de s'y préparer et d'y réagir.

La 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:

#### Gouvernance coordonnée

Les députés ont souligné qu'une coopération étroite et coordonnée est nécessaire entre le secteur public, le secteur privé, le monde universitaire, la société civile et les médias. En outre, la réponse de l'Union doit être coordonnée avec les institutions internationales ainsi qu'avec les partenaires internationaux de confiance qui partagent les mêmes valeurs. Afin de garantir la coopération avec des partenaires internationaux de confiance, ainsi que la protection contre les rivaux systémiques, les entités établies dans des pays tiers qui ne sont pas parties à l'accord de l'OMC sur les marchés publics (AMP) ne devraient pas être autorisées à participer à des marchés publics au titre du présent règlement.

#### Réserve de cybersécurité

En ce qui concerne la nouvelle réserve de cybersécurité, les députés soulignent qu'elle a le potentiel de développer les capacités industrielles dans l'UE, y compris pour les PME, grâce à des investissements dans la recherche et l'innovation qui permettront de développer des technologies de pointe, telles que les technologies de l'informatique en nuage et de l'intelligence artificielle. En outre, le rapport propose de conserver la participation des entreprises, de renforcer les critères et les garanties de fiabilité conditionnant leur participation (par exemple, une participation en association avec une entreprise nationale ou locale) en précisant les critères et la définition de la souveraineté technologique, ainsi que de s'assurer de l'équilibre entre acteurs de l'Union et de pays tiers. Il propose en outre un schéma de certification soit appliqué aux fournisseurs privés dans le cadre du mécanisme d'urgence dans le domaine de la cybersécurité pour bâtir des partenariats fiables et de long terme.

Pour soutenir la mise en place de la réserve de cybersécurité de l'UE, la Commission pourrait envisager de demander à l'ENISA de préparer un système de certification candidat pour les services de sécurité gérés dans les domaines couverts par le mécanisme d'urgence en matière de cybersécurité. Afin de remplir les tâches supplémentaires découlant de cette disposition, l'ENISA devrait recevoir un financement supplémentaire adéquat.

#### Financement

À la lumière des développements géopolitiques et du paysage croissant des cybermenaces, et afin d'assurer la continuité et le développement des mesures prévues dans le présent règlement au-delà de 2027, en particulier le bouclier européen de cybersécurité et le mécanisme d'urgence pour la cybersécurité, il est nécessaire de prévoir une ligne budgétaire spécifique dans le cadre financier pluriannuel pour la période 2028-2034. Selon le rapport, les États membres devraient s'efforcer de s'engager à soutenir toutes les mesures nécessaires pour réduire les cybermenaces et les incidents dans l'ensemble de l'Union et pour renforcer la solidarité.

#### Renforcer la R&I en matière de cybersécurité

Le texte amendé appelle à renforcer la recherche et l'innovation (R&I) dans le domaine de la cybersécurité afin d'accroître la résilience et l'autonomie stratégique ouverte de l'Union. De même, il est important de créer des synergies avec les programmes de R&I et avec les instruments et institutions existants et de renforcer la coopération et la coordination entre les différentes parties prenantes, y compris le secteur privé, la société civile, les universités, les États membres, la Commission et l'ENISA.

#### Évaluation et réexamen

Le texte modifié stipule que, dans un délai de deux ans à compter de la date d'application du présent règlement et tous les deux ans par la

suite, la Commission devrait procéder à une évaluation concernant, entre autres : i) une évaluation des points forts et des points faibles du mécanisme d'urgence pour la cybersécurité; ii) la contribution du présent règlement au renforcement de la résilience et de l'autonomie stratégique ouverte de l'Union, à l'amélioration de la compétitivité des secteurs industriels concernés, des microentreprises, des PME, y compris des jeunes pousses, et au développement des compétences en matière de cybersécurité dans l'Union; iii) l'utilisation et la valeur ajoutée de la réserve de cybersécurité de l'Union européenne.

## Mesures visant à renforcer la solidarité de l'Union et ses capacités de détection, de préparation et de réaction face aux menaces et aux incidents de cybersécurité

---

Le Parlement européen a adopté par 470 voix pour, 23 contre et 90 abstentions, une résolution législative sur la proposition de règlement du Parlement européen et du Conseil établissant des mesures destinées à renforcer la solidarité et les capacités dans l'Union afin de détecter les menaces et incidents de cybersécurité, de s'y préparer et d'y réagir.

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

### Objectifs

Le règlement proposé établit des mesures destinées à renforcer les capacités dans l'Union afin de détecter les menaces et incidents de cybersécurité, de s'y préparer et d'y réagir, notamment par les actions suivantes:

- établissement d'un réseau paneuropéen de cyberpôles («système européen d'alerte en matière de cybersécurité») dans le but de mettre en place et de développer des capacités de détection coordonnée et d'appréciation commune de la situation;
- la mise en place d'un mécanisme d'urgence dans le domaine de la cybersécurité pour aider les États membres et les autres utilisateurs à se préparer aux incidents de cybersécurité importants, majeurs et assimilés à des incidents majeurs, à y réagir, à en atténuer les retombées et à s'en rétablir;
- la mise en place d'un mécanisme européen d'analyse des incidents de cybersécurité afin d'analyser et d'évaluer les incidents importants ou majeurs.

Le règlement poursuit les objectifs généraux consistant à renforcer la position concurrentielle des secteurs de l'industrie et des services dans l'ensemble de l'économie numérique de l'Union, y compris les microentreprises et les petites et moyennes entreprises ainsi que les jeunes pousses, et à contribuer à la souveraineté technologique et à l'autonomie stratégique ouverte de l'Union dans le domaine de la cybersécurité, notamment en stimulant l'innovation dans le marché unique numérique.

Ces objectifs seront poursuivis en renforçant la solidarité au niveau de l'Union, en consolidant l'écosystème de cybersécurité, en accroissant la cyberrésilience des États membres et en développant les aptitudes, le savoir-faire, les capacités et les compétences de la main-d'œuvre dans le domaine de la cybersécurité.

Le règlement est sans préjudice des fonctions essentielles des États membres, notamment celles d'assurer l'intégrité territoriale de l'État, de maintenir l'ordre public et de préserver la sécurité nationale. En particulier, la sécurité nationale reste de la seule responsabilité de chaque État membre.

### Création du système européen d'alerte en matière de cybersécurité

Réseau paneuropéen d'infrastructures composé de cyberpôles nationaux et de cyberpôles transfrontières y adhérant sur une base volontaire, le système européen d'alerte en matière de cybersécurité sera mis en place pour soutenir le développement de capacités avancées permettant à l'Union de renforcer les capacités de détection, d'analyse et de traitement des données en rapport avec les cybermenaces et la prévention des incidents dans l'Union.

Lorsqu'un État membre décide de participer au système européen d'alerte en matière de cybersécurité, il désignera ou, le cas échéant, mettra en place un cyberpôle national. Les cyberpôles nationaux pourront coopérer avec des entités du secteur privé pour échanger des données et des informations pertinentes aux fins de la détection et de la prévention des cybermenaces et incidents, y compris avec les communautés sectorielles et transsectorielles d'entités essentielles et importantes.

### Cyberpôles transfrontières.

Lorsqu'au moins trois États membres s'engagent à veiller à ce que leurs cyberpôles nationaux collaborent pour coordonner leurs activités de détection des incidents de cybersécurité et de surveillance des cybermenaces, ces États membres pourront créer un consortium d'hébergement.

Un cyberpôle transfrontière est une plateforme multinationale établie par un accord de consortium écrit. Il sera conçu pour améliorer la surveillance, la détection et l'analyse des cybermenaces, pour prévenir les incidents et pour contribuer à l'obtention de renseignements sur les cybermenaces, notamment par l'échange de données et d'informations pertinentes et, le cas échéant, anonymes, ainsi que par le partage d'outils de pointe et le développement conjoint de capacités de détection, d'analyse, de prévention et de protection des cybermenaces dans un environnement de confiance.

### Mécanisme d'urgence

Un mécanisme d'urgence dans le domaine de la cybersécurité sera mis en place afin de favoriser l'amélioration de la résilience de l'Union face aux cybermenaces et d'anticiper et d'atténuer, dans un esprit de solidarité, les incidences à court terme d'incidents de cybersécurité importants, majeurs ou assimilés à des incidents majeurs.

Le mécanisme d'urgence soutiendra i) des actions de préparation, telles que des tests coordonnés de préparation des entités opérant dans des secteurs hautement critiques dans l'ensemble de l'Union, ii) d'autres actions de préparation pour les entités opérant dans des secteurs critiques; iii) les mesures prévues par les fournisseurs de services de sécurité gérés de confiance participant à la réserve de cybersécurité de

l'Union qui soutiennent la réaction aux incidents de cybersécurité importants, majeurs ou assimilés à des incidents majeurs et permettent d'amorcer le rétablissement suite à ces incidents; iv) les actions d'assistance mutuelle, apportée sous forme de subventions et aux conditions fixées dans les programmes de travail correspondants visés au règlement établissant le programme pour une Europe numérique.

#### Réserve de cybersécurité de l'UE

Une réserve de cybersécurité de l'Union sera créée afin d'aider, à leur demande, les utilisateurs à réagir aux incidents de cybersécurité importants, majeurs ou assimilés à des incidents majeurs, ou à fournir une assistance à cet effet, et à entreprendre le rétablissement immédiat après de tels incidents.

LENISA préparera, au moins tous les deux ans, une cartographie des services nécessaires aux utilisateurs des services de la réserve de cybersécurité. Les demandes d'aide adressées à la réserve de cybersécurité de l'UE seront transmises au pouvoir adjudicateur qui les évaluera. Une réponse sera transmise aux utilisateurs en tout état de cause, au plus tard 48 heures après la présentation de la demande afin de garantir l'efficacité de l'action de soutien. Le pouvoir adjudicateur informera le Conseil et la Commission des résultats du processus.

Un pays tiers associé au programme pour une Europe numérique pourra demander une aide à la réserve de cybersécurité de l'Union lorsque l'accord par lequel il est associé au programme pour une Europe numérique prévoit sa participation à la réserve.

#### Évaluation et réexamen

Au plus tard deux ans à compter de la date d'application du règlement et au moins tous les quatre ans par la suite, la Commission procédera à une évaluation du fonctionnement des mesures définies dans le règlement et présentera un rapport au Parlement européen et au Conseil.

Transparence				
GÁLVEZ Lina	Rapporteur(e)	ITRE	18/07/2024	ISACA
GÁLVEZ Lina	Rapporteur(e)	ITRE	28/02/2024	The Kangaroo Group
GÁLVEZ Lina	Rapporteur(e)	ITRE	16/01/2024	Deputy Permanent Representatives of Czechia and Slovakia to the EU
GROOTHUIS Bart	Rapporteur(e) fictif/fictive	ITRE	16/11/2023	CrowdStrike
GÁLVEZ Lina	Rapporteur(e) fictif/fictive	ITRE	15/11/2023	CrowdStrike
ALAMETSÄ Alviina	Rapporteur(e) fictif/fictive pour avis	TRAN	19/09/2023	Permanent Representation of the Netherlands to the EU
NIINISTÖ Ville	Rapporteur(e) fictif/fictive	ITRE	19/09/2023	Security Scorecard
GROOTHUIS Bart	Rapporteur(e) fictif/fictive	ITRE	14/09/2023	ESET, spol. s r.o.
GROOTHUIS Bart	Rapporteur(e) fictif/fictive	ITRE	13/09/2023	FOX IT
GROOTHUIS Bart	Rapporteur(e) fictif/fictive	ITRE	13/09/2023	VNO-NCW