

Règlement sur la cybersolidarité

En avril 2023, la Commission européenne a présenté une proposition de règlement 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 (règlement sur la cybersolidarité). Au cours de sa période de session d'avril II, le Parlement doit se prononcer sur l'accord conclu lors de négociations avec le Conseil.

Contexte

La guerre menée par la Russie contre l'Ukraine a révélé l'ampleur de notre dépendance à l'égard des technologies numériques et la fragilité de l'environnement numérique. Elle a déclenché une augmentation des [cyberattaques](#), qui ont un effet particulièrement perturbateur lorsqu'elles ciblent des infrastructures critiques – telles que l'[énergie](#), la [santé](#) ou les [services financiers](#) – qui dépendent de plus en plus des technologies, ce qui les rend plus efficaces mais également plus vulnérables aux perturbations informatiques. Dans ce contexte, la Commission a [présenté](#) une proposition de règlement sur la cybersolidarité, destinée à répondre à la nécessité urgente de 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 modification du [règlement établissant le programme pour une Europe numérique](#) permettrait le financement de la création d'un système d'alerte de cybersécurité («cyberbouclier») et d'un mécanisme d'urgence en matière de cybersécurité à l'appui des mesures de préparation, incluant une réserve de cybersécurité.

Position du Parlement européen

La commission de l'industrie, de la recherche et de l'énergie (ITRE) du Parlement a adopté son [rapport](#) en décembre 2023, en même temps qu'un mandat en vue d'engager des négociations interinstitutionnelles. Le Conseil a également arrêté sa [position](#) en décembre 2023. Les colégislateurs sont parvenus à un [accord](#) politique sur le texte en mars 2024. Le texte approuvé conserve les éléments de la proposition initiale de la Commission, tout en clarifiant et en élargissant certaines définitions, ainsi qu'en alignant les dispositions sur la législation existante, à savoir la [directive sur la sécurité des réseaux et des systèmes d'information \(directive SRI 2\)](#), afin d'éviter les redondances. Le règlement reposerait donc sur trois piliers:

- un **système** paneuropéen **d'alerte en matière de cybersécurité**, consistant en un réseau d'infrastructures de «**cyberpôles**», à la fois au niveau **national** (entités uniques établies par un État membre et agissant sous son autorité, qui peuvent coopérer avec des entités du secteur privé) et au niveau **transfrontière** (avec un consortium d'hébergement composé d'au moins trois États membres participants), qui partageraient des informations sur les cyberincidents afin de renforcer la résilience commune;
- un **mécanisme d'urgence en matière de cybersécurité**, comprenant une **réserve de cybersécurité** – un groupe d'entreprises privées (y compris des acteurs de pays tiers) offrant un soutien aux États membres (et à certains pays tiers) sur demande, afin de les aider en cas d'incident informatique important ou majeur;
- un **mécanisme d'analyse des cyberrisques**, au moyen duquel l'Agence de l'Union européenne pour la cybersécurité (ENISA), à la demande de la Commission ou du [réseau européen pour la préparation et la gestion des crises cyber](#) (EU-CyCLONE), analyse et évalue les menaces, les vulnérabilités exploitables constatées et les mesures d'atténuation relatives à des incidents importants ou majeurs, et produit un rapport d'analyse de l'incident contenant les enseignements tirés.

Le Parlement a obtenu que le développement des aptitudes, des capacités et des compétences de la main-d'œuvre figure au nombre des objectifs spécifiques de la proposition, et que l'ENISA se voie attribuer un rôle et des ressources accrues, en particulier en ce qui concerne la réserve de cybersécurité de l'Union.



Le Parlement a également obtenu que les fonds affectés à la réserve de cybersécurité ne compromettent pas d'autres objectifs du programme pour une Europe numérique, tels que les compétences numériques et l'intelligence artificielle.

Rapport en première lecture: [2023/0109\(COD\)](#); commission compétente au fond: ITRE; Rapporteuse: Lina Gálvez Muñoz (S&D, Espagne). Pour en savoir plus, consultez notre [briefing](#) «Législation européenne en marche» sur le sujet (en anglais).

[Conclusions de la conférence sur l'avenir de l'Europe](#): cette proposition présente un intérêt pour la proposition 28, mesures 1 et 2, et la proposition 33, mesure 3.

