Règlement sur la cybersécurité 2

2026/0011(COD) - 20/01/2026 - Document de base législatif

OBJECTIF : renforcer le cadre de cybersécurité de l’UE en réponse à l’évolution des cybermenaces, à la numérisation accrue et aux risques géopolitiques accrus affectant les chaînes d’approvisionnement des technologies de l’information et de la communication (TIC).

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 : depuis l’adoption du règlement (UE) 2019/881 du Parlement européen et du Conseil, les contextes géopolitique, technologique et réglementaire ont connu des transformations majeures. Les cyberattaques se sont multipliées et sont devenues plus sophistiquées, ciblant les infrastructures critiques, les entreprises et le grand public, avec les rançongiciels au cœur de ce phénomène. Les technologies émergentes telles que l’intelligence artificielle (IA) et l’informatique quantique redéfinissent les outils de défense et les tactiques des adversaires.

Cette proposition fait partie d'un ensemble de mesures visant à aligner le cadre de cybersécurité de l'Union sur les besoins des parties prenantes dans un contexte de menaces cybernétiques de plus en plus sophistiquées et de réalité géopolitique complexe.

CONTENU : la présente proposition révise le règlement (UE) 2019/881 qui définit le mandat et les missions actuels de **l’agence de l’Union européenne pour la cybersécurité** (ENISA) et du cadre européen de certification de cybersécurité (ECCF). Il est proposé que le mandat révisé de l'ENISA et les modifications apportées à l'ECCF soient établis dans le cadre d'un même instrument juridique, à savoir **un règlement**.

La proposition de révision du cadre de certification de la cybersécurité (CSA) vise clairement à **rationaliser, hiérarchiser et codifier les tâches relevant de la législation relative à la cybersécurité**. Une telle démarche ne peut être entreprise qu'au niveau de l'UE, et aucune initiative de ce type n'existe actuellement. La nouvelle proposition renforce la sécurité de la chaîne d'approvisionnement et le secteur de la cybersécurité au sein de l'UE, et améliore la préparation et la résilience des États membres et de l'industrie.

Plus précisément, le règlement vise à:

Renforcer le mandat et le rôle de l'ENISA en tant qu'agence de l'UE pour la cybersécurité

Depuis l'adoption de la première loi sur la cybersécurité en 2019, l'ENISA s'est imposée comme un pilier de l'écosystème de cybersécurité de l'UE. La loi révisée sur la cybersécurité permet à l'ENISA **d'aider l'UE et ses États membres à appréhender les menaces communes** et à se préparer aux cyberincidents, ainsi qu'à y réagir.

La proposition définit les missions de l'ENISA en matière de **coopération opérationnelle** avec les États membres, les entités de l'Union et le Service de cybersécurité pour les institutions, organes et organismes de l’Union (CERT-EU), le réseau des équipes d'intervention en cas d'incident de sécurité informatique (CSIRT), EU-CyCLONe et d'autres parties prenantes, notamment la publication de lignes directrices et la mise en œuvre d'outils de communication sécurisés. L'ENISA contribuera également à **améliorer la**

connaissance de la situation en matière de cybermenaces et d'incidents, notamment en développant un ou plusieurs référentiels de renseignements sur les cybermenaces, en effectuant des analyses et en émettant des alertes précoces.

Outre ces tâches, l'ENISA devrait fournir des outils et des plateformes, notamment une **plateforme unique de signalement**. L'Agence doit développer une capacité commune de service de gestion des vulnérabilités à l'échelle de l'Union et fournir des **services de gestion des vulnérabilités.**

L'ENISA continuera de jouer un rôle clé dans le développement des compétences en cybersécurité en Europe. Elle y parviendra en pilotant **l'Académie des compétences en cybersécurité** et en mettant en place des systèmes d'attestation des compétences en cybersécurité à l'échelle de l'UE.

Renforcer et étendre le cadre européen de certification de cybersécurité

La loi révisée sur la cybersécurité garantira que les produits et services destinés aux consommateurs de l'UE seront **testés plus efficacement** en matière de sécurité. Ceci sera réalisé grâce à un cadre européen de certification de cybersécurité (ECCF) renouvelé. L'ECCF apportera davantage de clarté et simplifiera les procédures, ce qui permettra d'élaborer des **systèmes de certification dans un délai de 12 mois par défaut**. Elle instaurera également une gouvernance plus souple et transparente afin de mieux impliquer les parties prenantes grâce à l'information et à la consultation publiques.

Les systèmes de certification, gérés par l'ENISA, deviendront **un outil pratique et volontaire** pour les entreprises. Ils leur permettront de démontrer leur conformité à la législation européenne, réduisant ainsi les contraintes et les coûts. Le cadre ECCF renouvelé constituera un atout concurrentiel pour les entreprises de l'UE. Pour les citoyens, les entreprises et les autorités publiques de l'UE, il garantira un niveau élevé de sécurité et de confiance dans les chaînes d'approvisionnement complexes des TIC.

Gérer les risques de cybersécurité liés aux chaînes d'approvisionnement des TIC

La nouvelle loi sur la cybersécurité vise à réduire les **risques liés aux fournisseurs de pays tiers** présentant des problèmes de cybersécurité dans la chaîne d'approvisionnement des TIC de l'UE. Elle établit un cadre de sécurité fiable pour cette chaîne d'approvisionnement, fondé sur une **approche harmonisée, proportionnée et axée sur les risques**. Ce cadre permettra à l'UE et aux États membres d'identifier et d'atténuer conjointement les risques dans les **18 secteurs critiques de l'UE**, en tenant compte également des impacts économiques et de l'offre du marché.

Le règlement sur la cybersécurité permettra un désengagement obligatoire des réseaux européens de télécommunications mobiles à l'égard de fournisseurs de pays tiers à haut risque, en s'appuyant sur les travaux déjà réalisés grâce à la boîte à outils pour la sécurité des réseaux 5G.

Renforcer la cohérence, l'efficacité et la résilience du cadre de cybersécurité de l'UE

La proposition définit les dispositions relatives aux **règles de délivrance des certificats européens de cybersécurité**, y compris ceux de niveau d'assurance «élevé». Elle établit également des règles d'harmonisation des systèmes européens de certification de cybersécurité avec les systèmes nationaux et prévoit la possibilité d'une **reconnaissance internationale des certificats européens**, fondée sur le principe d'équivalence. Des règles sont établies pour un **mécanisme d'évaluation par les pairs** entre les autorités, garantissant des normes équivalentes dans toute l'Union, ainsi que pour la coopération entre ces autorités au sein du Groupe européen de certification de cybersécurité (ECCG).

Incidences budgétaires

Le budget prévisionnel de l'ENISA s'élève à 341 millions d'euros sur sept ans, soit une moyenne annuelle de 49 millions d'euros (projection pour la période 2028-2034). Cela représente une augmentation de 81,5% par rapport au budget de l'Agence en 2025. Les avantages générés par cette initiative seront considérables, avec **des économies potentielles pour les entreprises pouvant atteindre 14,6 milliards d'euros**. Des mécanismes de financement ont été mis en place pour alimenter le budget de l'ENISA: les redevances perçues sur la délivrance des autorisations d'attestation de compétences, les redevances liées aux services d'outils de test et les redevances perçues pour la maintenance des systèmes européens de certification de cybersécurité. Le bénéfice attendu pour le budget de l'UE est estimé à environ **18,5 millions d'euros** sur la période 2028-2034.