Sécurité des réseaux et des systèmes d’ information (directive SRI 2) : simplification et alignement sur le « Cybersecurity Act 2 »

2026/0012(COD) - 14/01/2026 - Document de base législatif

OBJECTIF : simplifier la mise en œuvre de mesures visant à garantir un niveau élevé et commun de cybersécurité dans toute l'UE.

ACTE PROPOSÉ : Directive 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 : la directive (UE) 2022/2555 du Parlement européen et du Conseil relative à des mesures visant à assurer un niveau élevé et commun de cybersécurité dans l’ensemble de l’Union (directive NIS 2) établit des mesures destinées à garantir un niveau élevé et commun de cybersécurité dans toute l’Union, en vue d’améliorer le fonctionnement du marché intérieur. Depuis l’entrée en vigueur de la directive (UE) 2022/2555, des progrès ont été réalisés en matière de renforcement de la cyber-résilience de l’Union. Toutefois, sa mise en œuvre par les États membres a rencontré certaines difficultés, notamment concernant le champ d’application de la directive, l’application des obligations de gestion des risques de cybersécurité et de notification des incidents, ainsi que la supervision des entités transfrontalières.

S’appuyant sur la proposition de loi relative à la cybersécurité 2, des modifications ciblées devraient être apportées à la directive (UE) 2022/2555 afin de relever ces défis, en simplifiant certains aspects afin d’ accroître la sécurité juridique et d’assurer une mise en œuvre uniforme de la directive (UE) 2022/2555.

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 proposition de directive modifie la directive (UE) 2022/2555 (directive NIS 2) afin de simplifier sa mise en œuvre et d'assurer sa cohérence avec la future loi révisée sur la cybersécurité (loi sur la cybersécurité 2). Elle répond aux préoccupations exprimées par les États membres et les parties prenantes concernant la complexité administrative, les chevauchements entre les cadres de cybersécurité de l'UE et la nécessité d'une plus grande clarté juridique. Elle modifiera la directive NIS 2 existante et rationalisera davantage les obligations imposées aux entreprises, garantissant ainsi une harmonisation accrue au sein de l'Union.

L'objectif de la directive proposée devrait être considéré comme faisant partie des objectifs généraux du paquet de révision de la législation sur la cybersécurité, qui comprend la proposition de règlement du Parlement européen et du Conseil relatif à l'Agence de l'Union européenne pour la cybersécurité (ENISA), le cadre européen de certification de la cybersécurité et la sécurité de la chaîne d'approvisionnement des TIC, et abrogeant le règlement (UE) 2019/881.

Les principaux amendements ciblés à la directive NIS2 visent à:

- **faciliter la preuve de conformité à la directive NIS 2 par les entités et fournisseurs**: les entités régies par la directive NIS 2 pourront obtenir des certificats dans le cadre des systèmes organisationnels de

certification en cybersécurité développés dans le cadre de l'ECCF (cadre européen de certification en cybersécurité);

- **faciliter davantage le respect des mesures de gestion des risques de cybersécurité pour les entités multinationales soumises à la supervision des autorités compétentes de plusieurs États membres**: ENISA se verrait confier un nouveau rôle de soutien aux États membres dans la supervision de ces entités, la facilitation de l'entraide et la création d'une meilleure vue d'ensemble des entités relevant de la directive NIS 2.

Parmi les autres modifications ciblées figurent:

- des clarifications du **champ d'application et des définitions**. Certaines dispositions relatives au champ d'application concernant les prestataires de soins de santé, les producteurs d'électricité, les entreprises de production d'hydrogène et les entités du secteur chimique devraient être clarifiées afin de garantir la sécurité juridique et de réduire la charge de conformité pour les entités et les autorités nationales;

- **l'exclusion du périmètre** des fournisseurs de services DNS de petite et très petite taille;

- l'introduction d'une **harmonisation maximale des actes d'exécution** (spécifiant les mesures de gestion des risques de cybersécurité) afin de faciliter la conformité des entités et la supervision des autorités;

- l'introduction d'une **nouvelle catégorie de petites et moyennes capitalisations**; les entités qualifiées de petites et moyennes capitalisations seront désignées comme des entités importantes, réduisant ainsi leur charge de conformité et la charge de supervision des autorités compétentes;

- l'obligation pour les États membres d'adopter des politiques de **migration vers la cryptographie post-quantique (PQC)** dans le cadre de leur stratégie nationale de cybersécurité; et

- l'introduction d'une collecte harmonisée de données sur les **attaques de ransomware**.

Enfin, la proposition prévoit que la Commission adopte des **lignes directrices** sur l'application des exigences de sécurité de la chaîne d'approvisionnement que les entités relevant du champ d'application de la directive NIS 2 transmettent à leurs fournisseurs, afin de garantir la sécurité juridique et d'empêcher le transfert indu d'obligations à des entités ne relevant pas du champ d'application de la directive NIS 2.