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

2023/0109(COD) - 08/12/2023 - Rapport déposé de la commission, 1ère lecture/lecture unique

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 qu'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.