Résolution sur la stratégie de cybersécurité de l’ Union pour la décennie numérique

2021/2568(RSP) - 10/06/2021 - Texte adopté du Parlement, lecture unique

Le Parlement européen a adopté par 670 voix pour, 4 contre et 12 abstentions, une résolution sur la stratégie de cybersécurité de l’Union pour la décennie numérique.

Les députés ont rappelé que la transformation numérique - une priorité stratégique essentielle de l’Union - était inévitablement associée à une exposition accrue aux cybermenaces.

La crise de la COVID-19 a exacerbé les vulnérabilités informatiques dans certains secteurs critiques, en particulier les soins de santé, tandis que les mesures de télétravail ont accru la dépendance vis-à-vis des technologies numériques.

Le nombre de cyberattaques augmente considérablement et les menaces hybrides, qui comprennent le recours à des campagnes de désinformation et à des cyberattaques contre des infrastructures, des processus économiques et les institutions démocratiques, sont de plus en plus nombreuses et préoccupantes.

Produits connectés sécurisés et résilients aux cybermenaces

Les députés ont appelé à se fixer l’objectif de faire en sorte que tous les produits connectés à l’internet disponibles dans l’Union, ainsi que l’ensemble des chaînes d’approvisionnement qui les mettent à disposition, soient sécurisés dès leur conception, résilients aux cyberincidents et mis à jour dans les meilleurs délais lors de la découverte de vulnérabilités.

Le Parlement s’est félicité de l’intention de la Commission de proposer une législation horizontale sur les exigences en matière de cybersécurité applicables aux produits connectés et aux services associés. Il a demandé que cette législation prévoie l’harmonisation des législations nationales afin d’éviter la fragmentation du marché unique. Il a également invité la Commission à évaluer la nécessité d’une **proposition de règlement horizontal** qui introduise des exigences en matière de cybersécurité pour les applications, les logiciels, les logiciels intégrés et les systèmes d’exploitation d’ici à 2023.

Politiques en matière de cybersécurité

Soulignant la nécessité d’intégrer la cybersécurité dans la numérisation, le Parlement a demandé que les projets de numérisation financés par l’Union incluent des **exigences en matière de cybersécurité**. Il s’est félicité du soutien à la recherche et à l’innovation, en particulier en ce qui concerne les technologies de rupture (telles que l’informatique quantique et la cryptographie quantique) et a demandé la poursuite des recherches sur les algorithmes post-quantiques en tant que norme de cybersécurité.

Le Parlement a insisté pour que les politiques en matière de cybersécurité soient intégrées dans la stratégie numérique de l’Union et dans son financement, et pour qu’elles soient cohérentes et interopérables d’un secteur à l’autre. Il a recommandé une utilisation cohérente des fonds de l’Union en ce qui concerne la cybersécurité.

Infrastructures critiques

Le Parlement a insisté sur la nécessité de mettre en place un **nouveau cadre de sécurité** solide pour les infrastructures critiques de l'Union afin de préserver les intérêts de l'Union en matière de sécurité et de tirer parti des capacités existantes pour réagir de manière appropriée aux risques, aux menaces et aux changements technologiques.

Les députés ont invité la Commission à élaborer des dispositions visant à **garantir l'accessibilité, la disponibilité et l'intégrité du noyau public de l'internet** et, partant, la stabilité du cyberespace. Ils se sont félicités de la boîte à outils de l'Union sur la cybersécurité de la 5G et ont invité la Commission, les États membres et les acteurs du secteur à poursuivre leurs efforts en faveur de réseaux de communication sécurisé.

Résilience stratégique de l'Union

La Commission et les États membres sont invités à **mettre leurs ressources en commun** afin de renforcer la résilience stratégique de l'Union, de réduire sa dépendance à l'égard des technologies étrangères et de promouvoir son leadership et sa compétitivité en matière de cybersécurité tout au long de la chaîne d' approvisionnement numérique, y compris le stockage et le traitement des données dans le nuage, les technologies des processeurs, les circuits intégrés (puces), la connectivité ultrasécurisée, l'informatique quantique et la prochaine génération de réseaux.

La résolution a souligné la nécessité d'un **cadre de sécurité solide et cohérent** pour protéger l'ensemble du personnel, des données, des réseaux de communication et des systèmes d'information de l'Union, ainsi que les processus décisionnels contre les cybermenaces, et l'importance de fonder ce cadre sur des règles globales, cohérentes et homogènes ainsi qu'une gouvernance appropriée.

Les députés ont invité la Commission et les États membres à renforcer la confiance et à réduire les obstacles au partage d'informations sur les cybermenaces et les cyberattaques à tous les niveaux.