LOI SUR LA CYBER-RESILIENCE

Proposition COM(2022) 454 du 15 septembre 2022 de **règlement relatif aux exigences horizontales en matière de cyber-sécurité applicables aux produits comportant des éléments numériques** et modifiant le règlement (UE) 2019/1020.

Analyse du cep No. 1/2023

VERSION COURTE

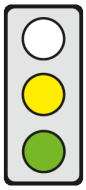
Contexte | Objectif | Parties intéressées

Contexte : Ces dernières années, les produits logiciels et matériels ont été de plus en plus sujets à des cyberattaques. L'une des principales causes est le faible niveau de cyber-sécurité de ces produits. Rien qu'en 2021, des pertes s'élevant à 5 500 milliards d'euros ont été enregistrées dans le monde. La Commission propose donc une loi sur la cyber-résilience (Cyber Resilience Act - CRA).

Objectif : La Commission souhaite établir des règles de cyber-sécurité uniformes pour les fabricants, importateurs et distributeurs de produits comportant des éléments numériques (PEN). Les fabricants de PEN doivent améliorer la cyber-sécurité de leurs produits dès la phase de conception et de développement. En outre, la transparence concernant les caractéristiques de sécurité des PEN doit être renforcée.

Parties concernées : Fabricants, importateurs, distributeurs et utilisateurs de PEN, organismes d'évaluation de la conformité.

Brève évaluation



Pour

- La loi sur la cyber-résilience apporte une contribution importante au renforcement de la cyber-sécurité dans l'UE. Elle remédie, de manière ciblée, à plusieurs déficits sur les marchés des PEN.
- Des exigences uniformes en matière de cyber-sécurité contrecarreront les fausses incitations des fabricants, importateurs et distributeurs de PEN, qui doivent désormais supporter une part plus importante des coûts liés aux PEN non sécurisés. Il sera plus difficile de répercuter ces coûts sur les clients et les tiers.
- Les exigences en matière de transparence permettront aux acheteurs de véhicules à moteur diesel d'évaluer et de comparer plus facilement leurs caractéristiques de sécurité.
- La fixation d'un calendrier pour la correction des vulnérabilités donne aux utilisateurs de PEN une plus grande confiance dans la qualité du produit.

Contre

- La classification des produits critiques en deux classes, déjà entreprise par la Commission, est non transparente et incohérente. Il existe des PEN dans les deux classes qui ne peuvent être considérés comme critiques en soi.
- La classification des PEN en fonction de leur criticité ne peut être considérée comme une décision purement technique exempte de considérations politiques. La délégation de pouvoirs à la Commission pour adopter des actes délégués sur la classification est donc au moins discutable.
- La date de début envisagée - 2 ans après l'entrée en vigueur de la CRA - est trop ambitieuse.

Évaluation générale

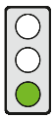
Proposition de la Commission : Un cadre juridique pour le développement et la distribution de produits cyber-sécurisés avec des éléments numériques (PEN) sera établi dans l'UE.

Auteurs : Anastasia Kotovskaia, LL.M. et Philipp Eckhardt | kotovskaia@cep.eu
cep | Kaiser-Joseph-Strasse 266 | 79098 Freiburg | Téléphone +49 (0)761 38693-0 | www.cep.eu
Traduction : Mathilde Baudouin | cepfrance@cep.eu

Evaluation du cep : Les fabricants de PEN sortent régulièrement des produits qui ne sont pas cyber-sécurisés. Dans le même temps, il est difficile pour les acheteurs de PEN d'exiger des produits sûrs en raison de divers déficits sur les marchés des PEN, tels que de fausses incitations du côté des fabricants et un manque d'informations disponibles pour les acheteurs. L'ARC apportera une contribution tangible et significative à la résolution de ces déficits du marché.

Exigences uniformes en matière de cyber-sécurité

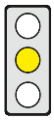
Proposition de la Commission : Les fabricants, importateurs et distributeurs de PEN devront se conformer aux exigences de base en matière de cyber-sécurité. Une attention suffisante doit déjà être accordée à la cyber-sécurité lors des étapes de conception, de développement et de fabrication d'un produit.



Evaluation du cep : Des exigences uniformes en matière de cyber-sécurité contrecarreront les fausses incitations parmi les fabricants, importateurs et distributeurs de PEN. A l'avenir, ils devront investir davantage dans la cyber-sécurité de leurs produits. Cela permettra de réduire les coûts que les clients et les tiers ont souvent dû supporter jusqu'à présent à cause de PEN non sécurisés. En outre, les désavantages concurrentiels subis par les acteurs économiques qui sont proactifs dans la fourniture de produits sûrs seront réduits, et le parasitisme entre les acheteurs de PEN sera plus difficile.

Portée

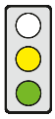
Proposition de la Commission : L'ARC s'applique aux produits comportant des éléments numériques (PEN). Il s'agit, notamment, de produits logiciels ou matériels connectables. Les PEN sont divisés en quatre groupes : (1) les PEN non critiques, notamment les disques durs et les jeux informatiques, (2) les PEN critiques (classe I), notamment les navigateurs et les gestionnaires de mots de passe, (3) les PEN critiques (classe II), notamment les systèmes d'exploitation pour serveurs, les routeurs et les cartes à puce, et (4) les PEN hautement critiques non encore spécifiés.



Evaluation du cep : Définir le champ d'application comme très large est approprié car les vulnérabilités peuvent se produire dans de nombreux PEN, même supposés non critiques. Cependant, la classification des produits critiques en 2 classes, qui a déjà été entreprise, manque de transparence. En outre, la classification est incohérente car il existe de nombreux PEN dans les deux classes qui ne peuvent pas toujours être considérés comme critiques en soi. En fait, leur criticité dépend de l'endroit où ils sont utilisés, par qui et dans quelles conditions.

Gestion des vulnérabilités

Proposition de la Commission : Les fabricants de PEN doivent s'assurer que les vulnérabilités sont traitées pendant la durée de vie prévue du produit ou pendant cinq ans à compter de la date de mise sur le marché du produit, la période la plus courte étant retenue.



Evaluation du cep : La fixation d'un délai pour que les fabricants corrigent les vulnérabilités donne aux utilisateurs de PEN une plus grande confiance dans la qualité des produits. Cependant, la cohérence avec d'autres législations européennes, concernant la durée de l'obligation de corriger les vulnérabilités, n'est pas encore en place, notamment vis-à-vis de la proposition de directive sur la responsabilité du fait des produits défectueux et des nouvelles exigences d'éco-conception pour les smartphones, tablettes et téléphones mobiles.

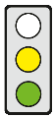
Exigences de transparence

Proposition de la Commission : Les fabricants d'EDP doivent fournir des informations aux utilisateurs des produits, telles que les circonstances dans lesquelles des risques de cyber-sécurité peuvent survenir lors de l'utilisation des PEN, la durée pendant laquelle les mises à jour de sécurité seront fournies, et le point de contact de l'entreprise où les informations sur les vulnérabilités peuvent être signalées.

Evaluation du cep : Les exigences de transparence permettent aux consommateurs et aux entreprises de classer et de comparer plus facilement les caractéristiques de sécurité des PEN. Cela leur permet de prendre une décision éclairée quant à l'acquisition d'un PEN. Ces exigences contribuent donc à réduire les défaillances du marché causées par les asymétries d'information.

Exigences en matière de rapports

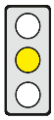
Proposition de la Commission : Les fabricants de PEN doivent signaler tout incident de cyber-sécurité ou toute vulnérabilité activement exploitée à l'Agence de l'Union européenne pour la cyber-sécurité (ENISA) dans les 24 heures.



Evaluation du cep : Les fabricants de PEN sont souvent réticents à signaler volontairement les incidents ou les vulnérabilités en matière de cyber-sécurité en raison des risques pour leur réputation. Cependant, ces rapports présentent souvent un avantage économique majeur, car des mesures peuvent être prises pour réduire le risque à un stade plus précoce. Les obligations de signalement sont donc appropriées. Néanmoins, l'obligation de notifier toute vulnérabilité exploitable ou tout incident de sécurité est excessive. Comme pour la ligne directrice NIS 2, leur importance doit être prise en compte.

Classification des PEN en fonction de leur criticité

Proposition de la Commission : La Commission peut, au moyen d'actes délégués, ajouter de nouvelles catégories de produits critiques aux listes de PEN critiques ou supprimer des catégories de ces listes. Ainsi, elle peut également créer une liste avec des catégories de PEN hautement critiques. Sa décision se fonde sur plusieurs critères, comme le fait que le PEN soit utilisé par des opérateurs d'infrastructures critiques.



Evaluation du cep : Le fait que la Commission puisse créer des listes de PEN (hautement) critiques par le biais d'actes délégués signifie que ses décisions manquent de transparence. De plus, le degré auquel les critères doivent être remplis n'est pas précisé. Une telle délégation de pouvoir à la Commission engendre un risque que la classification des PEN soit influencée par des considérations politiques.

Auteurs : Anastasia Kotovskaia, LL.M. et Philipp Eckhardt | kotovskaia@cep.eu
cep | Kaiser-Joseph-Strasse 266 | 79098 Freiburg | Téléphone +49 (0)761 38693-0 | www.cep.eu
Traduction : Mathilde Baudouin | cepfrance@cep.eu