Législation sur la cyberrésilience

Des baby-moniteurs aux montres intelligentes, les produits et logiciels qui contiennent un composant numérique sont omniprésents dans notre vie quotidienne. Moins évident pour de nombreux utilisateurs est le risque de sécurité que ces produits et logiciels peuvent présenter.

Le règlement sur la cyberrésilience (CRA) (https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act) vise à protéger les consommateurs et les entreprises qui achètent des produits logiciels ou matériels comportant un composant numérique. Le règlement sur la cyberrésilience s'attaque au niveau inadéquat de cybersécurité de nombreux produits et à l'absence de mises à jour de sécurité en temps utile pour les produits et les logiciels. Il s'attaque également aux défis auxquels les consommateurs et les entreprises sont actuellement confrontés lorsqu'ils tentent de déterminer quels produits sont cybersécurisés et de les configurer en toute sécurité. Les nouvelles exigences faciliteront la prise en compte de la cybersécurité lors de la sélection et de l'utilisation de produits contenant des éléments numériques. Il sera plus simple d'identifier les produits matériels et logiciels dotés des fonctionnalités de cybersécurité appropriées.

Le règlement sur la cyberrésilience introduit des exigences obligatoires en matière de cybersécurité pour les fabricants et les détaillants, régissant la planification, la conception, le développement et la maintenance de ces produits. Ces obligations doivent être respectées à chaque étape de la chaîne de valeur. La loi oblige également les fabricants à fournir des soins pendant le cycle de vie de leurs produits. Certains produits critiques présentant un intérêt particulier pour la cybersécurité devront également faire l'objet d'une évaluation par un tiers par un organisme agréé avant d'être vendus sur le marché de l'UE.

Le règlement s'applique à tous les produits connectés directement ou indirectement à un autre dispositif ou réseau, à l'exception des exclusions spécifiées telles que certains logiciels ou services open source déjà couverts par les règles existantes, comme c'est le cas pour les dispositifs médicaux, l'aviation et les voitures. Les produits porteront le**marquage CE** (https://single-market-economy.ec.europa.eu/single-market/ce-marking_en) pour indiquer qu'ils sont conformes aux exigences de l'ARC. Les nouvelles règles rééquilibreront la responsabilité à l'égard des fabricants, qui doivent veiller à ce que leurs produits comportant des éléments numériques répondent aux normes de cybersécurité pour le marché de l'UE. Cela permettra aux acheteurs de prendre des décisions plus éclairées, en faisant confiance à la cybersécurité des produits marqués CE.

Le règlement sur la cyberrésilience est entré en vigueur le 10 décembre 2024. Les principales obligations introduites par la loi s'appliqueront à partir du 11 décembre 2027.

En outre, le groupe d'experts de la législation sur la cyberrésilience (groupe d'experts de l'ARC) (https://ec.europa.eu/transparency/expert-groups-register/screen/expert-groups/consult?lang=en&groupID=3967) est en cours de création. Le groupe d'experts assistera et conseillera la Commission sur les questions relatives à la mise en œuvre de la législation sur la cyberrésilience.

Le règlement sur la cyberrésilience s'appuie sur lastratégie de cybersécurité de l'UE de 2020 etla stratégie (https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy) de l'UE pour l'union de la sécurité. (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX%3A52020DC0605&from=EN) Il complète d'autres actes législatifs dans ce domaine, en particulier ladirective SRI 2. (https://digital-strategy.ec.europa.eu/en/policies/nis-directive)
