Adoption du réglement sur la cyberrésilience (*Cyber Resilience Act* ou *CRA*) : application progressive avec des premières obligations en matière de sécurité pour les produits numériques dès l'été 2026

En octobre, le Conseil de l'Union européenne a adopté le règlement relatif aux exigences de cybersécurité applicables aux produits comportant des éléments numériques qui constitue l'un des piliers de la stratégie de l'Union européenne en matière de cybersécurité aux côtés des directives NIS 2, DORA ainsi que l'*AI Act*. Le CRA a été publié au Journal officiel de l'Union européenne le 20 novembre dernier.

Le règlement sur la cyberrésilience vise à instaurer un standard de cybersécurité uniforme à l'échelle européenne pour les produits logiciels et matériels comportant des éléments numériques, c'est-à-dire tous les produits qui sont directement ou indirectement connectés à un autre dispositif ou à un réseau (objets connectés tels que caméras, téléviseurs, montres intelligentes, ordinateurs, jeux vidéo, jouets, produits de l'internet des objets (« IoT »), etc.). En effet, ces produits sont la cible de nombreuses cyberattaques, impactant la sécurité, la vie privée et la santé des consommateurs de l'Union européenne (« UE »).

L'objectif de ce règlement est double : (i) le développement sécurisé des produits comportant un élément numérique en s'assurant que les matériels et logiciels soient mis sur le marché comportent moins de vulnérabilités et que les fabricants prennent au sérieux la sécurité tout au long du cycle de vie des produits et (ii) permettre aux consommateurs de prendre en compte la cybersécurité dans la sélection et l'utilisation de ces produits, ce qui sera notamment facilité par le marquage « CE ».

Ce règlement définit ainsi des exigences de sécurité applicables à l'ensemble des acteurs de la chaîne d'approvisionnement (fabricant, distributeur et importateur) pendant toute de la durée de vie de ces produits (conception, développement, production, mise à disposition sur le marché). A cet effet, le texte établit une liste de critères spécifiques auxquels les produits comportant des éléments numériques fabriqués ou distribués dans le marché européen devront répondre.

Ainsi, cela peut expliquer que le fait que les définitions de certaines notions clés comme « vulnérabilité » et « incident » sont issues de la directive NIS 2 et servent de référence pour la définition des critères de sécurité des produits. En outre, l'amélioration du niveau de cybersécurité des produits contenant des éléments numériques faciliterait la mise en conformité des entités relevant du champ d'application de la directive NIS 2 et à terme renforcerait la sécurité de l'ensemble de la chaîne d'approvisionnement.

Le champ d'application du texte est vaste puisqu'il concerne à la fois les produits qui peuvent être connectés physiquement via des interfaces matérielles et les produits qui sont connectés logiquement, à l'exception de ceux déjà couverts par des règles de cybersécurité spécifiques (tels que les dispositifs médicaux, les produits aéronautiques, les voitures).

A défaut de respecter ces exigences, ces derniers s'exposeront à des amendes administratives ainsi qu'à des obligations de retrait ou rappel des produits non conformes. Les sanctions seront prononcées par une autorité nationale de surveillance désignée par chaque État membre.

Les nouvelles obligations s'appliqueront à compter du 11 décembre 2027 sauf exceptions (notamment celles de notification des vulnérabilités et incidents incombant aux fabricants qui seront applicables à partir du 11 septembre 2026).

Lien utile :

- Règlement concernant des exigences horizontales en matière de cybersécurité pour les produits comportant des éléments numériques (règlement sur la cyberrésilience), 10 octobre 2024