Accédé le 01 août 2025 via l'URL:

https://www.usine-digitale.fr/article/cyber-resilience-act-comment-s-y-preparer.N2235893

Cyber Resilience Act : comment s'y préparer ?

29 juillet 2025

Entré en vigueur il y a six mois, le Cyber Resilience Act pose un cadre européen harmonisé pour la cybersécurité des objets connectés. Cette chronique de Maître Pascal Agosti de Caprioli & Associés met en avant les éléments saillants de ce texte pilier majeur de la stratégie de l'UE en matière de cybersécurité.

L'ensemble des produits connectés de la vie quotidienne (domotique, objets intelligents, dispositifs interconnectés) sont autant de vecteurs potentiels de cyberattaques. Le Cyber Resilience Act, entré en vigueur le 10 décembre 2024, a pour objectif principal de renforcer la cybersécurité de ces derniers en établissant un cadre européen harmonisé des règles applicables et ce, dès la conception de ces

produits ou lors de leur mise sur le marché.

A qui s'adresse-t-il ?

Le Cyber Resilience Act (CRA) s'adresse à **toute personne mettant à disposition sur le marché européen un produit contenant des éléments numériques**. Il s'agit **du fabricant du produit mais aussi de l'importateur et/ou le distributeur mettant à disposition sur le marché de l'Union européenne ledit produit** et ceci, indépendamment de ses origines géographiques. En ce sens, il concerne aussi bien les opérateurs économiques établis au sein de l'UE que les extra-européens.

A quoi s'applique-t-il ?

Le CRA s'applique à un large éventail de produits numériques dont l'utilisation prévue ou raisonnablement prévisible implique une connexion directe ou indirecte, logique ou physique, à un appareil ou à un réseau, qu'il s'agisse d'hardwares ou de softwares.

Des exceptions existent comme les logiciels Open Source distribués sans objectif commercial, les équipements marins ou encore les pièces de rechange sous certaines conditions…De plus, **tout produit et matériel comportant des éléments numériques faisant déjà l'objet d'un règlement sont exclus du champ d'application**. Il en va notamment ainsi pour les dispositifs médicaux, les véhicules à moteur ou bien encore l'aviation civile (règlements UE 2017/745 et 746 ; UE 2018/1139 si produits certifiés ; et UE 2019/2144).

Une approche par les risques

Le CRA conserve une **approche par les risques**, dépendant de la typologie de produit contenant des éléments numériques (art. 10). En l'occurrence, le risque est analysé au regard de **la criticité des produits**, c'est-à-dire de l'incidence que peut avoir une vulnérabilité dans un tel produit. Ainsi a été pris en considération : la sensibilité de l'environnement ; l'utilisation pour une finalité critique ou sensible tel que le traitement de données à caractère personnel ; l'accès administrateur à des fonctionnalités réseau ; l'ampleur potentielle ou réelle d'un incident de cybersécurité

sur ledit produit (art. 6).

Cette approche permet de responsabiliser toute la chaîne de distribution du produit, pour éviter que l'utilisateur final ou une autorité judiciaire ne puisse engager la responsabilité d'un opérateur hors de l'Union en cas de non-conformité. **L'importateur et le distributeur doivent garantir la conformité du produit à chaque étape de la distribution, comme dans toute réglementation similaire.**

Compliance by design

La conformité des produits contenant des éléments numériques doit passer par **une approche de la sécurité dès la conception du produit et durant tout le cycle de vie de ce dernier** (art. 10). Cette évaluation doit porter aussi bien sur les risques inhérents aux accès réseau qu'à la gestion des données traitées par le produit (Annexe 1, sect. 1). Cette approche, tout à fait classique en la matière, appelle à effectuer en amont **une évaluation des risques des produits contenant des éléments numériques**. Cette analyse permet de comprendre les enjeux lors du développement et de prévoir tous les aspects techniques et administratifs à mettre en place pour la bonne conformité à cette nouvelle règlementation.

Sécurité et transparence vis-à-vis de l'utilisateur

Le Cyber Resilience Act aborde également la question de la sécurité **sous l'angle organisationnel**. Le fabricant est soumis à une **obligation de diligence pour effectuer la détection et le traitement des vulnérabilités**. Les vulnérabilités doivent être gérées "efficacement" et de manière conforme à l'annexe 1, section 2.

L'article 10 traite des "aspects pertinents de la cybersécurité", ce qui inclut notamment les vulnérabilités (Ann. I, sect. 2). Cette obligation relativement floue (art. 2) requiert des lignes directrices permettant aux entreprises productrices de produits contenant des éléments numériques, de cibler les informations pertinentes pour les autorités.

Le fabricant devra être en mesure de **pouvoir faire remonter toute information**

concernant une vulnérabilité qui toucherait un de ses produits et qui serait activement exploitée ou non (art. 11). La transparence demandée au fabricant lors d'un incident n'est cependant pas chose aisée, puisqu'il importe aussi de ne pas divulguer d'information compromettante qui permettrait à de potentielles personnes malveillantes d'utiliser les informations publiques afin de profiter d'une vulnérabilité qui ne serait pas encore corrigée.

Déclaration UE de conformité

Un autre élément de cette transparence est **l'obligation de déclaration UE de conformité**. En effet, les fabricants de produits contenant des éléments numériques devront apposer sur leur produit un marquage CE (art. 20). À cette fin, ils devront mettre en œuvre la documentation précisée à l'art. 23 du règlement qui permet de prouver les moyens mis en œuvre par le fabricant pour se mettre en conformité avec le règlement, ainsi que se référer à la législation spécifique au **marquage CE** (Règl. (CE) n° 765/2008, 9 juill. 2008, art. 3).

Evaluation des produits

Afin d'assurer la sécurité des produits contenant des éléments numériques, il reviendra aux fabricants **d'évaluer leur produit au regard des exigences essentielles mentionnées à l'annexe I**. Cette évaluation est différente selon que le produit est considéré comme un produit "important" de classe I ou II, au sens de l'annexe III, en fonction de sa fonctionnalité principale ("core functionality").

Les produits non listés à l'annexe III, ainsi que les produits importants de classe I intégralement conformes à des "normes harmonisées" (qui sont en cours de rédaction à ce stade) couvrant toutes les exigences applicables, peuvent faire l'objet d'une autoévaluation de conformité. Dans ce cas, le fabricant établit la documentation technique, rédige une déclaration UE de conformité sous sa seule responsabilité, et appose le marquage CE sur le produit. En revanche, les produits importants de classe II sont soumis à une évaluation obligatoire par un organisme notifié, conformément à l'article 32(3).

Par ailleurs, les produits critiques **visés à l'annexe IV pourront être soumis à un schéma européen de certification de cybersécurité, selon les modalités précisées par actes délégués. Ces mécanismes de conformité visent à garantir un niveau de sécurité élevé et à assurer la transparence des fabricants vis-à-vis des utilisateurs et des autorités compétentes**. Ces évaluations ont une double utilité : forcer la mise en conformité, d'une part, et la transparence des fabricants vis-à-vis des utilisateurs, d'autre part.

Quelles sanctions ?

Si le fabricant ne se conforme pas aux dispositifs du règlement, les autorités de contrôle des marchés désignées par les États membres prendront des sanctions à leur encontre. Les sanctions restent tout à fait classiques au regard des standards européens et s'inscrivent donc dans la continuité (art. 53) :

- violation des critères de conformité ou des obligations du fabricant : jusqu'à 15 millions d'euros ou 2,5 % du CA annuel total ;
- violation de toute autre obligation du règlement : jusqu'à 10 millions d'euros ou 2 % du CA annuel total ;
- fourniture d'informations incomplètes, incorrectes ou trompeuses à l'organisme d'évaluation du produit ou à l'autorité de surveillance du marché : jusqu'à 5 millions d'euros ou 1 % du CA annuel total ;
- produit non conforme ou présentant un risque aux yeux de l'autorité de surveillance du marché : restriction, suspension ou interdiction de la disponibilité du produit sur le marché.

Quel calendrier ?

L'application du Cyber Resilience Act sera progressive :

- **11 juin 2026 : entrée en vigueur des dispositions relatives aux organismes d'évaluation de la conformité ;**

- **11 septembre 2026 : début de l'application des obligations de notification des vulnérabilités activement exploitées et des incidents graves à la charge des fabricants ;**
- **11 décembre 2027 : applicabilité de toutes les dispositions du CRA.**

Quelles actions ?

Les entreprises doivent se préparer en identifiant avec soin la qualification appropriée de tous leurs produits connectés ainsi que les obligations afférentes applicables dans un environnement réglementaire pluriel. Quid en effet en cas de superposition de réglementation avec l'AI Act ? Se préparer à ce nouveau paradigme nécessitera de passer par des acteurs spécialisés en la matière et des plateformes innovantes permettant l'automatisation et la simplification des processus de conformité. Ces outils permettent d'accélérer la réalisation des évaluations techniques, la gestion proactive des vulnérabilités et la documentation de conformité.

Pascal Agosti, avocat associé, docteur en Droit

Caprioli & Associés, membre du Réseau JurisDéfi