Cyber Resilience Act : les enjeux pour les fabricants et éditeurs de produits connectés

Par Frédéric Forster, avocat à la cour d'appel de Paris

La défense européenne passe inévitablement aujourd'hui par la cybersécurité. C'est pourquoi l'Europe met en place la loi sur la cyberrésilience, qui vise à établir des normes communes pour renforcer les règles en matière de vulnérabilité numérique.

« Si tout est connecté, tout peut être piraté. Comme les ressources sont rares, nous devons unir nos forces. [...] C'est pourquoi nous avons besoin d'une politique de cyberdéfense européenne, notamment d'une législation établissant des normes communes dans le cadre d'une nouvelle loi européenne relative à la cyberrésilience. » Des propos forts, tenus par la présidente de la Commission européenne, Ursula von der Leyen, lors de son discours sur l'état de l'Union 2021, qui a mis en avant à quel point la cybersécurité et la cyberdéfense revêtent aujourd'hui une dimension géostratégique. La Commission européenne a notamment identifié deux problèmes majeurs :

- un faible niveau général de cybersécurité ;
- l'absence d'intelligibilité, voire l'absence pure et simple, des informations qui permettraient aux consommateurs de privilégier des produits sécurisés ou de les utiliser de façon sécurisée.

Cette prise de conscience de la Commission l'a conduite à créer un cadre législatif plus abouti concernant entre autres les objets connectés. Ainsi, la proposition de règlement, connue sous le nom de « loi sur la cyberrésilience » ou Cyber Resilience Act (CRA), définit notamment deux objectifs principaux :

- créer les conditions nécessaires au développement de produits sûrs comportant des éléments numériques, en veillant à ce que les matériels et les logiciels soient mis sur le marché avec moins de vulnérabilité et veiller à ce que les fabricants prennent la sécurité au sérieux tout au long du cycle de vie d'un produit ;
- créer des conditions permettant aux utilisateurs de tenir compte de la cybersécurité lors de la sélection et de l'utilisation de produits comportant des éléments numériques.

Certains produits seraient exclus car leur cybersécurité est déjà encadrée par d'autres règlementations, tels des dispositifs médicaux à usage humain, des accessoires à ces dispositifs, des dispositifs médicaux de diagnostic *in vitro* à usage humain et de leurs accessoires.

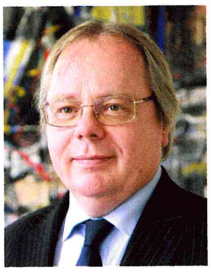
Le CRA comporte trois corps de règles :

- celles relatives à la mise sur le marché de produits comportant des éléments numériques afin de garantir leur cybersécurité. Ces produits numériques ne pourront être mis à disposition sur le marché qu'à la condition de satisfaire aux exigences essentielles du règlement et que si les processus des fabricants sont conformes aux exigences essentielles du règlement ;
- celles relatives à ces exigences essentielles, depuis la conception en passant par le développement et la production de ces produits, qui seront classés en fonction de la criticité du risque cyber qu'ils comportent ;
- enfin, celles relatives aux obligations qui incomberont spécifiquement aux fabricants, importateurs et distributeurs de ces produits.

Dans certains cas de criticité élevée, les fabricants devront faire appel à un organisme tiers pour l'évaluation de la conformité du produit concerné. Enfin, les États membres désigneront une « autorité notifiante » responsable de la mise en place et de l'application des procédures nécessaires à l'évaluation et à la notification des organismes d'évaluation de la conformité ainsi qu'au contrôle des organismes notifiés.

Les sanctions pour non-respect des exigences essentielles pourront s'élever à 15 millions d'euros ou à 2,5 % du chiffre d'affaires annuel mondial total, le montant le plus élevé étant retenu.

Ce texte n'en est qu'à l'étape d'un projet, qui doit encore passer par la procédure d'adoption par le Parlement européen et le Conseil pour entrer en vigueur. Après son entrée en vigueur, une période de transition de vingt-quatre mois est prévue pour permettre aux acteurs concernés de se mettre en conformité.



BIO EXPRESS

Avocat à la cour d'appel de Paris, Frédéric Forster dirige, depuis 2006, le pôle Télécoms du cabinet Alain Bensoussan Avocats Lexing. Il était précédemment directeur juridique du groupe SFR. Il est aussi vice-président du réseau international d'avocats Lexing.