Sécurité de l'IoT : l'UE esquisse son Cyber Resilience Act

À votre avis, quel est, sur une échelle de 1 à 5, le niveau global de cybersécurité des produits numériques commercialisés dans l'UE ? C'est sur cette question que s'ouvre la première section d'une consultation publique à ce sujet. En ligne de mire, un texte que la Commission européenne envisage d'adopter dans le courant du 3e trimestre 2022 : le **Cyber Resilience Act**. Il prendrait la forme d'une législation horizontale (transsectorielle) encadrant la mise sur le marché des produits en question et des services dont ils dépendent. Ursula von der Leyen y avait appelé lors du dernier discours sur l'état de l'Union. Le Conseil de l'Europe avait suivi.

Bruxelles a choisi de viser large avec sa consultation. Autant sur la portée (ouverte à tout public) que sur le contenu, divisé en quatre sections.

Parmi les éléments abordés dans la première section :

– Évaluation de l'impact des incidents sur ces produits au niveau des organisations et des utilisateurs

– Capacité des fournisseurs à traiter les enjeux et intégrer la cybersécurité à chaque étape de développement des produits

– Attentes des consommateurs, dont obligations contractuelles

La deuxième section invite à évaluer l'efficacité de diverses mesures. Elles vont d'un système de certification volontaire à des bonnes pratiques en direction des acheteurs. En passant par l'ajout d'une dimension numérique dans des textes existants.

La Commission européenne s'interroge justement sur la pertinence des textes existants. Plus particulièrement trois d'entre eux :

– Directive de 2001 relative à la sécurité générale des produits
– Directive de 2006 relative aux machines
– Acte délégué d'octobre 2021 complétant la directive de 2014 sur les équipements radio pour préciser son applicabilité à certains types de produits

Security by design, *by default* ou les deux ?

Toujours dans la deuxième section, Bruxelles cherche à déterminer quel périmètre encadrer : tous les logiciels ou uniquement l'embarqué ? seulement le matériel exposé à un certain niveau de risque ?… Et cherche aussi à savoir ce qui peut le mieux contribuer à renforcer la sécurité parmi, notamment :

– Intégration à toutes les étapes de la conception (*security by design*)
– Activation d'usine (*security by default*)

– Traçabilité des composants (SBOM)
– Capacité à mettre à jour les produits

Autre enjeu de la consultation : mesurer l'opportunité d'une législation européenne par rapport à des législations nationales. Ce en évaluant, notamment, les coûts de mise en conformité. Mais aussi les bénéfices pour le marché intérieur : sécurité renforcée face à des risques sans frontières, rééquilibrage concurrentiel, sensibilisation des utilisateurs finaux…

Régulation de l'IoT : des bases en Europe… et en France

En matière d'encadrement des dispositifs connectés, on ne part pas de rien. Parmi les pièces maîtresses, il y a le Cybersecurity Act de 2019. Le texte définit un cadre pour harmoniser les méthodes d'évaluation et les niveaux d'assurance de la certification de cybersécurité. Il accompagne les travaux de l'ENISA (Agence européenne chargée de la sécurité des réseaux et de l'information). Laquelle a déjà élaboré un socle potentiel, en l'objet de schémas applicables aux services cloud.

En France, le Sénat avait adopté, en 2018, une résolution européenne sur la régulation de l'IoT. Elle appelait l'UE à mettre rapidement en place une certification des objets connectés incluant :

– Capacité de désactivation sélective ou totale
– Possibilité de mises à jour de sécurité
– Usage de technologies cryptographiques

Bien qu'elle semble privilégier une approche européenne, la France ne part pas non plus de rien. Elle a notamment son Code de la consommation. Le Parlement a déjà suggéré de l'adapter pour « prévoir quels opérateurs de services aux personnes par l'intermédiaire d'objets connectés sont tenus de délivrer à ces personnes une information loyale, claire et transparente sur les conditions générales d'utilisation de ces services ».

Photo d'illustration © garrykillian – Adobe Stock