Juliette Hulot
Marie-Lou Minel

Cyber Resilience Act : Quels changements ?

« Si tout est connecté, tout peut être piraté » disait Ursula Van Der Leyen, présidente de la Commission européenne, en 2021.

2021

DISCOURS
prononcé par Ursula Van Der Leyen
Déjà, elle exprimait la nécessité d'une politique de cyberdéfense

13/03/22

CONSULTATION PUBLIQUE
lancée par la Commission européenne pour recueillir les avis et expériences des parties prenantes

05/22

ANNONCE
de la publication à venir au troisième trimestre 2022

15/09/22

PUBLICATION DE LA PROPOSITION
visant à réglementer la sécurité des objets connectés et des produits numériques
Objectifs :
→ trouver une solution à l'insécurité juridique puisque les mesures prises au niveau international et européen sont hétérogènes
→ Rééquilibrer sur le plan cyber la relation contractuelle qui est souvent défavorable au consommateur

L'article 2 de la proposition indique qu'elle s'applique aux produits à composante numérique dont l'utilisation actuelle ou raisonnablement prévisible comporte une connexion directe ou indirect, physique ou logicielle, à un réseau ou à un autre appareil.
Exemples : un smartphone, un ordinateur, une télévision connectée, un aspirateur robot…

La proposition vise aussi des produits dits « critiques » qui représentent 10% des produits visés

2 sous-catégories selon le niveau de criticité

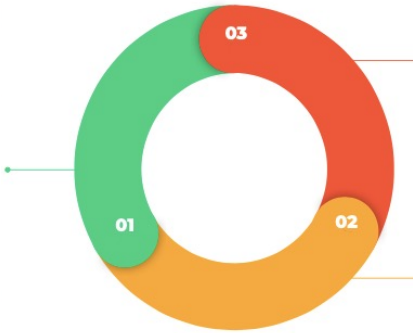
RÔLE CENTRAL DANS LA SÉCURITÉ DU RÉSEAU
Anti-virus, gestionnaire de mots de passe…

RISQUE POUR BEAUCOUP DE PERSONNES
Systèmes d'exploitation, logiciels de gestion des services cloud…

Exclusions

SONT EXCLUS
les dispositifs dans le domaine médical* et aéronautique** (déjà couverts par d'autres réglementations européennes) et les services en ligne (pas directement liés à un produit)

Exemples de risques prévenus



RISQUE D'ESPIONNAGE
via les jouets connectés pour enfants

EXPLOITATION PAR DES CYBERCRIMINELS
des données des caméras de surveillance connectées

*Règlement EU 2017/745
**Règlement EU 2018/1139

Conséquences et efficacité du règlement

NOUVELLES OBLIGATIONS (ARTICLES 10 À 14)

OBLIGATION DE CONTRÔLER LA CYBERSÉCURITÉ

1. **Évaluation des risques** à considérer dès la conception (F, I).

2. **Diligence** lors de l'intégration de composants tiers et lors de la mise sur le marché (F & D).

3. Surveiller les **vulnérabilités potentielles** du produit lors de sa mise sur le marché, pendant sa durée de vie et pendant 5 ans après sa mise sur le marché.

4. Établir / s'assurer de l'établissement d'une **documentation technique** avec **évaluation de conformité** à la disposition des autorités pendant 10 ans après la mise sur le marché (F, I).

5. Prendre des **mesures correctives** voire **retirer** le produit du marché en cas de non-conformité lors de sa mise sur le marché, pendant la durée de vie du produit et pendant 5 ans après la mise sur le marché (F, I & D).

6. S'assurer que les autres acteurs ont respecté leurs obligations (I & D).

OBLIGATIONS D'INFORMATION

1. Communiquer / s'assurer de la communication d'un **document technique** (F, I & D).

2. Fournir aux **utilisateurs** des **informations** sur le produit et des **instructions** et les informer en cas d'**incident** (F).

3. **Prouver la conformité** et mettre en place les **mesures requises** en cas de demande motivée de l'autorité de contrôle. L'informer en cas de suspicion de non-conformité (F, I & D).

4. Informer l'Agence de l'Union européenne pour la cybersécurité sous 24h en cas de connaissance de la vulnérabilité d'un produit et informer les mesures correctives prises le cas échéant (F, I & D).

5. Informer les **autorités** de contrôle et les **utilisateurs** du produit de l'éventuelle **cessation d'activité** du fabricant du produit (I & D).

CONSÉQUENCES PRATIQUES

PRÉCISIONS SUR LE CARACTÈRE DILIGENT

1. La diligence implique une attention « raisonnablement censée » vis-à-vis du consommateur relativement aux pratiques de marché honnêtes et au principe de bonne foi posé par la directive du 11 mai 2005. Le consommateur doit être parfaitement informé afin qu'il puisse donner son consentement en tout état de cause.

→ Référence à une pratique commerciale loyale.

LA CRÉATION D'UN ORGANISME CERTIFIANT

2. Afin de se conformer aux nouvelles obligations du règlement, il semble indispensable d'avoir recours à un organisme certifiant.

→ Contraignant en termes de moyens humains, financiers et de compétences de se mettre en conformité en interne.

En conséquence, des organismes de contrôle devraient naître dans les mois et années à venir, de même qu'une certification qui y serait affiliée.
Le recours à cette procédure devrait être la première procédure utilisée par les destinataires du Cyber Resilience Act.

Par « diligence », la disposition entend un devoir de sensibiliser le consommateur sur le fait que son comportement peut lui être préjudiciable même en ayant une utilisation du produit conforme aux instructions.

APPROCHE CRITIQUE

DES CONSÉQUENCES FINANCIÈRES DISPROPORTIONNÉES ?

1. À qui incombera la charge du financement de l'organisme certifiant ?

→ Il est fort probable que le coût du recours à l'organisme soit répercuté sur le fabricant qui augmentera dès le départ le coût du service ou de la chose.

2. Par enchainement, l'importateur fera de même, ce qui signifie que le dernier maillon de la chaîne de la consommation devra débourser une somme plus importante : le consommateur.
Le règlement qui devait pousser à la consommation en raison d'une meilleure sécurité risque de se heurter à la réalité économique des consommateurs et de l'inflation actuelle.
Les acteurs seront-ils prêts à mettre le montant nécessaire afin de s'assurer une meilleure sécurité ?

UN INTÉRÊT DÉJÀ EXPÉRIMENTÉ AVEC LA POUPÉE CONNECTÉE "CAYLA" PLEBISCITÉE PAR LES ENFANTS

Cayla est une poupée capable d'émettre et d'enregistrer des sons. Elle est contrôlable à distance avec un téléphone portable. Un tiers peut écouter l'enfant et lui parler à travers la poupée en se connectant via Bluetooth. Aucun code d'accès n'est requis et aucune notification n'est envoyée aux parents.
En décembre 2022, l'UFC a saisi la CNIL de la question suivante : que deviennent les données collectées par la poupée ? Il s'est avéré que les conditions contractuelles autorisent les sociétés à collecter et transmettre lesdites données.
La poupée connecter Cayla est alors un réel outil d'espionnage et la réalité des risques qu'elle présente a déjà conduit à l'interdiction à la vente en Allemagne.

Quelles sanctions en cas de non-conformité ?

Deux sanctions sont prévues par la proposition

L'INTERDICTION DE LA COMMERCIALISATION

En cas de non-conformité, interdiction de commercialisation sur le sol européen du produit faisant l'objet de failles de cybersécurité.
Une telle interdiction peut affecter significativement l'activité :

1. Perte de rentabilité
2. Perte de productivité
3. Perte de réputation

DES AMENDES

Les États membres devront veiller à respecter les règles de cybersécurité. En cas d'échec → amende pouvant aller jusqu'à 15M d'euros ou 2,5% du chiffre d'affaires mondial de l'entreprise concernée.
S'ils ne respectent aucune autre obligation prévue par la réglementation → amende pouvant aller jusqu'à 10 millions d'euros ou 2% du chiffre d'affaires mondial.
S'ils fournissent des informations incorrectes, incomplètes ou trompeuses aux autorités de contrôle → amende pouvant aller jusqu'à 5 millions d'euros ou 1% de leur chiffre d'affaires mondial.

Délai de 2 ans pour se mettre en conformité.

Les prochaines étapes

D'ici à 2024

1. Vote par le Parlement européen
2. Vote par le Conseil de l'Union européenne
3. Application aux États membres une fois votée

Délai de mise en conformité