



L'loT : des menaces persistantes mais des réponses juridiques émergentes

Garance Mathias - [@GaranceMathias](https://twitter.com/GaranceMathias)

IoT & Sécurité, Etat des lieux

© 2018, de nombreuses attaques via des IOT

- du véhicule électrique à Amazon Echo.

© Constats :

- Tous les secteurs d'activités, de l'industrie sont concernés
- La sécurité doit être intégrée dans l'IOT (security by design)

Intelligence artificielle, quelles perspectives dans l'UE ?



© Communication de la Commission au Parlement européen, au Conseil européen, au Conseil, au Comité économique et social européen et au Comité des régions - L'intelligence artificielle pour l'Europe - 25 Avril 2018

- La Commission a prévu d'accroître ses investissements de 2,5 milliards d'euros jusqu'en 2027.
- L'UE dans son ensemble – tant le secteur public que privé – devrait également augmenter ses investissements en matière de recherche et d'innovation d'au moins 20 milliards d'euros avant 2020.
- L'une des raisons principales de cette initiative est le fait que l'UE veuille concurrencer la Chine et les Etats-Unis. En effet, ces deux pays déploient des moyens considérables :
 - 970 millions d'euros dans la recherche non confidentielle en matière d'IA en 2016 pour les Etats-Unis (selon la Commission européenne),
 - 59,07 milliards de dollars d'ici 2025 pour la Chine qui ambitionne de devenir le leader mondial dans le secteur (selon les chiffres du Gouvernement chinois).

Intelligence artificielle, quelles perspectives dans l'UE ?



- © La Commission devrait bientôt publier sa propre interprétation de la **directive sur la responsabilité du fait des produits**, « à la lumière de l'évolution technologique ».

- © La Commission a prévu de procéder au réexamen des cadres juridiques existants, notamment :
 - la directive relative aux machines,
 - la directive sur les équipements radioélectriques,
 - la directive sur la sécurité générale des produits,
 - les règles spécifiques en matière de sécurité sur les dispositifs médicaux ou les jouets par exemple,
 - les règles relatives à l'interopérabilité.

Intelligence artificielle, quelles perspectives dans l'UE ?



- © Résolution du Parlement européen en date du 16 février 2017 contenant des recommandations à la Commission concernant des règles de droit civil sur la robotique EC/2015/2103(INL), adoptée à une très large majorité
- Le Parlement demande d'envisager la création « *d'une personnalité juridique spécifique aux robots, pour qu'au moins les robots autonomes les plus sophistiqués puissent être considérés comme des personnes électroniques responsables, tenues de réparer tout dommage causé à un tiers (...)* ».
 - Le Parlement requiert « *une clarification des règles et des critères applicables à l'utilisation des caméras et des capteurs embarqués dans les robots dans le cadre de la mise en œuvre du RGPD* ».

IoT & Sécurité, exigence du législateur californien

- © Nouvelle législation relative aux objets connectés en date du 28 septembre 2018
 - Entrée en vigueur au 1er janvier 2020
- © **Obligation principale** : implémenter des mesures de sécurité raisonnables dans tous les objets connectés distribués en Californie
 - Mesures de sécurité à adapter selon la nature et les fonctionnalités des objets connectés / selon les informations qui peuvent être collectées, stockées ou transmises
 - **Similitudes avec le principe de privacy by design** : conception des objets de manière à ce que les informations qu'ils contiennent ne puissent pas être accessibles à des tiers non autorisés, ni utilisés, détruites, modifiées ou divulguées.
 - Informations au sens large, pas seulement les données personnelles

IoT & Sécurité, exigence du législateur californien

- © Pas d'exemple concret donné par le législateur californien quant aux mesures de sécurité raisonnables
- © **Seule obligation prévue expressément** :
 - Mot de passe unique pour chaque objet connecté ou mécanisme imposant à l'utilisateur de créer un nouveau moyen d'authentification qui lui soit personnel avant toute utilisation de l'objet connecté

© Limites expressément prévues dans la loi :

- Les agences gouvernementales peuvent obtenir des informations de la part d'un fabricant d'objets connecté
- Les particuliers ne peuvent pas engager une action
 - Les seuls habilités à faire appliquer ces mesures sont énumérés dans la loi (procureur général, etc.).

Références



- © <https://www.techrepublic.com/article/5-biggest-iot-security-failures-of-2018/>
- © https://leginfo.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB327
- © https://leginfo.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB1906
- © <https://ec.europa.eu/transparency/regdoc/rep/1/2018/FR/COM-2018-237-F1-FR-MAIN-PART-1.PDF>
- © <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2017-0051+0+DOC+XML+V0//FR>