SECURITE DE L'IOT

Les objets connectés saisis par le droit

Salon des industries du futur

Mulhouse Parc des expositions 14 juin 2017

Me Alexandre NAPPEY, avocat associé

La collecte de données par les objets connectés est-elle entourée de garanties suffisantes ?

DONNEES COLLECTEES

- Données personnelles
- Données sensibles
- Données biométriques
- Données de trafic et de connexion
- Métadonnées

ENJEUX & RISQUES

- Marché des données personnelles et algorithmes prédictifs
- Droit au respect de la vie privée
- Droit à l'oubli
- Piratage des objets connectés

PRINCIPES

- Finalité
- Proportionnalité
- Durée de conservation des données
- Transparence
- Respects des droits de l'utilisateur

LE REGLEMENT EUROPEEN

- Renforcement des pouvoirs de sanction de la CNIL
- Obligation pour les entreprises de mener une étude d'impact du traitement envisagé sur la vie privée
- L'approche *privacy by design*

Quelles sont les règles applicables en cas de cyberattaque ?

ABSENCE D'INFRACTION AD HOC

- Il n'existe pas encore d'infraction spécifique aux objets connectés,
- La doctrine s'interroge sur l'opportunité d'un droit pénal spécial des objets connectés,

LES OBLIGATIONS DES ACTEURS

- **Article 34 de la loi informatique et Libertés** : les responsables de traitement doivent « *prendre toutes précautions utiles permettant de préserver la sécurité des données* ».

LES RESSOURCES DU DROIT PENAL

- **Article L. 323-1 du code pénal** : L'accès ou maintien **frauduleux** dans tout ou partie d'un système de traitement automatisé de données (STAD) est puni de deux ans d'emprisonnement et de 60 000 euros d'amende.
- **Article L. 323-3 du code pénal** : Le fait d'introduire frauduleusement des données dans un système de traitement automatisé, d'extraire, de détenir, de reproduire, de transmettre, de supprimer ou de modifier frauduleusement les données qu'il contient est puni de cinq ans d'emprisonnement et de 150 000 € d'amende.
- Les difficultés liées à l'auteur de l'infraction.
- Les difficultés liés à l'application du droit international aux conflits cyber technologiques.

Quels sont les régimes de responsabilité applicables aux objets connectés ?

LA DEFAILLANCE DE L'OBJET CONNECTE

- L'impossible application de l'article 1242 nouveau du code civil
  - L'utilisateur de l'objet connecté qui **en perd le contrôle et la direction** ne peut être tenu responsable du dommage causé par celui-ci.
  - **L'autonomie** de l'objet connecté et les problématiques liées à **l'intelligence artificielle**

- L'application difficile du régime de la responsabilité des produits défectueux de l'article 1245 du code civil.
  - Les difficultés liées à **l'identification de la composante défaillante**
  - Les difficultés liées au ***machine learning***

LA RESPONSABILITE DU FABRIQUANT

- Délit d'obsolescence programmée (art. L. 441-2 du code de la consommation) : réduire par des mesures volontaires la durée de vie d'un objet.

VERS UNE RESPONSABILITE SANS FAUTE

- Une responsabilité sans faute pourrait permettre l'indemnisation quasi-automatique de la victime.

- La responsabilité retenue pourrait être celle des créateurs des traitements algorithmés des objets connectés.

CLAIRMONT
Avocats

Pour nous contacter

CLAIRMONT Avocats

Tél.: +33 (0)1.56.79.55.80 Fax.: +33 (0)1.56.79.55.81

Paris
9, rue Pierre le Grand
75008 Paris

Bordeaux
103, avenue Georges Mandel
33000 Bordeaux

Strasbourg
5, place du Corbeau
67000 Strasbourg

www.clairmont-avocats.com

