16 juin 2016

Droit et cybersécurité des objets connectés

François Coupez
Avocat à la Cour, associé

Droit des nouvelles technologies, de l'informatique et de la communication
Chargé d'enseignement à l'Université de Paris II Panthéon-Assas, au CELSA

Assiste et conseille les entreprises en droit des nouvelles technologies / propriété intellectuelle

Marques, Brevets, Dessins & Modèles, Nom de domaine et droit d'auteur, Innovation et transformation numérique, Sécurité des SI, Données personnelles, Contrats informatiques, Dématérialisation, E-commerce, Evaluation, gestion et protection du patrimoine informationnel et actif immatériel, etc.

SPÉCIALISTE

Analyse juridique rigoureuse

Certificat de spécialisation en droit des nouvelles technologies, de l'informatique et de la communication

+

Compréhension du fonctionnement technique

+

Orientation business

- ✓ **Anticiper les problématiques juridiques pour mieux les gérer**
- ✓ **Proposer des solutions juridiques innovantes prenant en compte l'ensemble des impératifs**

La cybersécurité des objets connectés… une priorité ?

- Une multiplication du nombre des objets et de leur diversité (drones, capteurs d'activité, balances, ampoules, lunettes, voitures, etc.)
- Une sécurité rarement pensée dès l'origine
- Une mise à niveau souvent compliquée
- Des exemples de piratage toujours plus nombreux
- Une surface de risque en augmentation constante

De nombreux textes applicables… sans les viser strictement et notamment…

- Loi Godfrain du 5 janvier 1988 relative à la fraude informatique
- Loi de 1978 sur la protection des données personnelles
- Règlement « données personnelles **» - RGPD**
- Règlement « identification électronique et services de confiance »
- Projet de Directive « NIS » (Network and information security)
- Projet de Loi pour une République numérique
- Les textes propres à l'écosystème de l'objet connecté (transport, santé, etc.)

Des textes pour réprimer les atteintes… et des textes pour imposer leur sécurisation

Le renforcement des sanctions contre les cyber-criminels

- La loi Godfrain du 5 janvier 1988 relative à la fraude informatique : l'objet connecté est un STAD !

- ✓ Des incriminations au large spectre d'efficacité
- ✓ En 2004, lutte contre détention indue des solutions servant au piratage (y compris publication des moyens d'exploiter les failles)
- ✓ En 2012, circonstance aggravante si cible = système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat

Le renforcement des sanctions contre les cyber-criminels

- ✓ En 2014, pénalisation du « vol d'informations » extraites d'un SI
- ✓ Une sanction plus forte que le vol physique !
- ✓ En 2015, forte aggravation des peines
- ✓ L'art. 11 du projet de loi « renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale »

Une volonté politique forte sans cesse réaffirmée, une application très mesurée par les tribunaux…

La loi de 1978 : protéger les données personnelles collectées

- ✓ Difficile d'imaginer un objet connecté sans penser « donnée personnelle » (mais pas impossible)
- ✓ L'article 34 et l'obligation de sécurité des données – art. 226-17 du Code pénal
- ✓ Les sanctions actuelles de la CNIL
- ✓ La question des données de santé
- ✓ Des limites, dont législateurs français et européen sont conscients
- ✓ Le renforcement des sanctions de la CNIL par le projet de loi numérique
  - ✓ **1 500 000 € (x10)**
  - ✓ **Information des personnes de l'existence de la sanction, aux frais de l'entreprise sanctionnée**

Focus sur le Règlement européen sur la protection des données à caractère personnel (RGPD ou GDPR)

- ✓ Un texte structurant, **applicable dès le 25 mai 2018**
- ✓ Un enjeu de société
- ✓ Une application mondiale en principe

- ***L'***accountability : l'enjeu de la conformité
- L'analyse d'impact, les exigences fortes en matière de sécurité, l'interconnexion de fichiers, les **notifications des violations de sécurité**, les droits des personnes, les labels, etc.
- La **coresponsabilité du sous-traitant**
- Privacy by design… et **Legal by design ?**

Accountability du RGDP : que le règne de la conformité vienne

- **Faire ne suffit pas, il faut prouver que l'on a :**
  - ✓ **Evalué objectivement les risques de chaque traitement** pour les droits et libertés des personnes physiques **et mis en œuvre les mesures adaptées (analyse de risque)**
  - ✓ **Rédigé des règles internes et des procédures strictes sur tous les aspects du traitement**
  - ✓ **Conservé les traces documentaires**
  - ✓ **Conservé les instructions données au sous-traitant et prévu de strictes clauses contractuelles** (également à destination des sous-sous-traitant éventuels)
  - ✓ **Fait appliquer ces règles (audits, etc.)**
  - ✓ **Réalisé les études d'impact pour certains traitements**

Une traçabilité de tous les instants

Responsabilité ... et co-responsabilité

Aujourd'hui : le donneur d'ordre est le responsable du traitement, pas de délégation de responsabilité

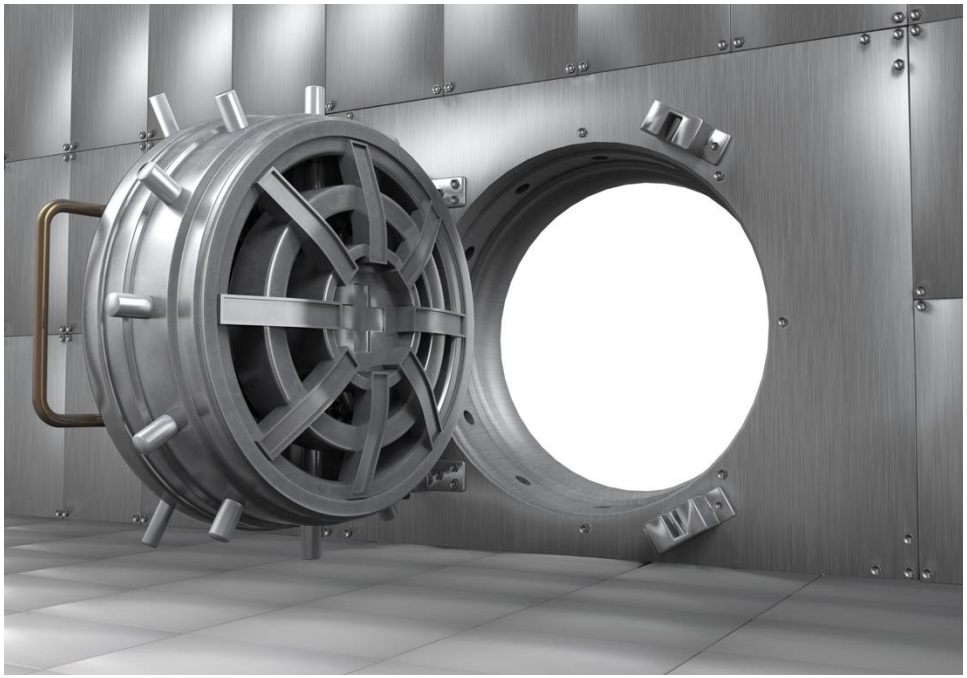
- Application des règles difficiles par exemple vis-à-vis de certains prestataires US…

Avec le Règlement : le donneur d'ordre est le responsable du traitement… mais le prestataire peut devenir **co-responsable**…

- Les nécessaires garanties du sous-traitant comme conditions de choix par le client
- Une sous-sous-traitance encadrée strictement
- Une assistance pour les aspects sécurité et pour le respect des droits d'accès, etc.
- La voie contractuelle pour la distinction des rôles
- Une assistance pour la preuve des obligations… les audits et les inspections !

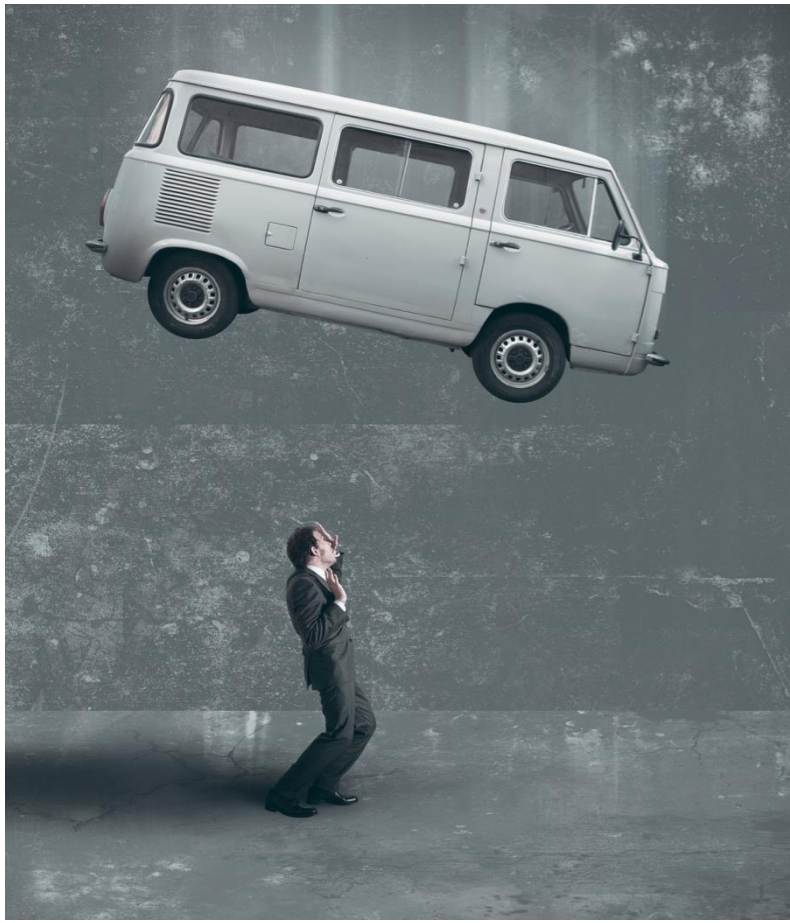
Aspect sécurité : on rappelle et précise ce qui est connu

- Articles 32 à 34 – section spécifique
- Mesures techniques et organisationnelles appropriées, compte tenu du risque (précédemment analysé)
- Des exemples donnés : pseudonymisation, chiffrement, procédure PDCA, etc.



Des sanctions qui changent non plus de monde, mais d'univers

Des sanctions pécuniaires de jusqu'à 10 M€ / 20 M € ou, dans le cas d'une entreprise, jusqu'à **2% / 4 % du CA « annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu »**



Une évolution probable grâce au RGPD

- **Renforcement de la sécurité globale**
- **Meilleure connaissance de la menace**
- Renforcement du **contrôle des sous-traitants… donc des fabricants et distributeurs d'objets connectés**
  - ✓ Du fait des risques de lourdes sanctions
  - ✓ Et **surtout liée à la co-responsabilité de ces derniers**
- **La barrière à l'entrée liée au** privacy by design
- **La certification et les labels ad hoc comme avantages concurrentiels**

La conformité pour renforcer la confiance des clients

En attendant, la pression sur les entreprises (fabricants, distributeurs, utilisatrices etc.) prend de multiples formes

- Quand la CNIL transforme l'obligation de moyens en obligation de résultat : 12/06/2014, sanction de DHL
- **20 sanctions publique de la CNIL pour défauts de sécurité ces 30 derniers mois**
- Les obligations sectorielles (secteur de la santé, transports, etc.)
- **Les conséquences de l'utilisation au sein de l'entreprise : BYOCL = BYOD²**
- **L'utilisation des données générées : big data, impact sur le droit de la preuve, ...**

Rappel sur les conséquences annexes d'un défaut de sécurisation des objets connectés distribués

- 19/03/2014, la Cour de cassation bouleverse sa jurisprudence établie
- **Une cybersécurité insuffisante diminue le droit à réparation du préjudice de la victime**
- Cela dépend de l'appréciation de la faute de la victime par les magistrats…
- Un impact sur les assurances cyber...

Vers une quadruple peine pour l'entreprise en cas de piratage des objets connectés distribués …

1. **Toutes les conséquences négatives « classiques » liées au piratage** (pertes, efforts de remédiation, indisponibilité, effets d'image, procès, voire actions de groupe, etc.)

2. **En cas de données personnelles accédées, risque CNIL de constatation d'un défaut de sécurité**

3. **Si un défaut de sécurité a permis le piratage, diminution des dommages intérêts en conséquence**

4. **Et risques de sanctions diverses (pénales ? A terme surtout 2% CA mondial + notation financière en berne)**

Avez-vous des questions ?

Merci de votre attention !

François COUPEZ

Avocat à la Cour, Associé

Droit des nouvelles technologies, de l'informatique et de la communication

f.coupez@atipic.legal

31, boulevard Malesherbes, 75008 Paris
01 80 48 11 25

@f_coupez

Technologies
Informations
Propriété
Intellectuelle
Communication