Objets connectés

Lunettes, lave-linge, téléviseurs, montres, systèmes de vidéosurveillance, serrure, fourchette, etc., autant d'objets électroniques connectés qui partagent aujourd'hui notre quotidien. Qu'ils soient directement connectés au *Web* en *wifi* ou bien par l'intermédiaire d'un *smartphone* (avec lequel ils communiquent en *Bluetooth*), ces objets prennent une nouvelle dimension. Le consommateur connecté peut ainsi surveiller sa maison, la distance qu'il a parcourue dans la journée et son rythme cardiaque en deux clics sur l'écran de son *smartphone*.

Aujourd'hui, les objets connectés sont partout. Ils sont dans l'automobile, dans la salle de bain avec la brosse à dents, dans la cuisine avec le réfrigérateur qui peut lister par lui-même les aliments manquants ou périmés, et même dans le monde de la mode. Les objets connectés de cette catégorie sont aussi appelés des «***Wearables***», ou «***Wearable Computing***» (en français : informatique vestimentaire), soit des interfaces informatiques que l'on porte sur le corps

Un marché en pleine expansion
La vente des **objets connectés a doublé en** 2014, atteignant 150 millions d'euros. Les bracelets, les montres connectées et de sport (avec le *GPS*), ont **représenté la majorité des ventes d'objets connectés en France, aux alentours de 90 millions d'euros**.
On estime qu'il se vendra environ **2 milliards d'objets connectés au cours des 5 prochaines années en France**. Ils seront vendus principalement en grandes surfaces spécialisées (GSS) et sur le *web*. Près de 640.000 clients se sont laissés séduire par ce type d'accessoires en 2014.

Outre nos téléphones, nous sommes entourés d'objets communicants et intelligents. Dans le commerce, ce sont des étiquettes *RFID* pour lutter contre la fraude, gérer les stocks ou, bientôt, pour contrôler le contenu de tout un *caddy* à la caisse. Dans nos immeubles, ce sont les capteurs de relevés de compteurs qui informent l'exploitant des consommations en temps réel.

Une vigilance nécessaire de la part des consommateurs

L'explosion des objets connectés expose principalement les consommateurs à deux types de risques :

- l'utilisation commerciale des données personnelles et les atteintes à la vie privée.

Une des conséquences de ce monde de réseau et de communication est que nous laissons de plus en plus de traces numériques. Au-delà des progrès technologiques, il s'agit désormais de parvenir à garantir l'anonymat des données : un tout autre *challenge.* Les objets communicants reçoivent, interprètent et communiquent entre eux les données préalablement collectées.

En 2010 déjà, un industriel spécialiste de la domotique affirmait avoir «*la technologie pour* enregistrer chaque minute, *chaque seconde, chaque microseconde, plus ou moins en direct, etc. Partant de là, nous pouvons déduire combien de personnes sont présentes dans la maison, ce qu'elles font, (etc.) : des quantités de données privées*».

Non seulement les entreprises spécialisées sont ainsi capables de suivre votre vie quotidienne à la trace mais elles sont aussi en mesure d'en tirer les conséquences au niveau de votre mode de vie et de votre santé en particulier.

« Le scénario dans lequel une assurance santé ou une mutuelle conditionnerait l'obtention d'un tarif avantageux à l'accomplissement d'un certain nombre d'activités physiques, chiffres à l'appui, se dessine.» Extrait du rapport de la CNIL mai 2014 « *Le corps, nouvel objet connecté* ».
De même, il est tout à fait envisageable que la collecte de ces données puisse déboucher sur certaines formes de discrimination, discrimination à l'embauche par exemple, ou discrimination par le prix si les données recueillies ont mis en évidence un niveau de revenus important chez un consommateur.

- Les risques de piratage

Dès lors que «se connecter à internet» devient une fonction intégrante des grille-pain, pèse-personnes et lave-vaisselle, les concepteurs de ces équipements doivent gérer un nouveau genre de problèmes, un genre qu'ils n'avaient jamais eu à envisager jusqu'alors, celui des *cybers* attaques.

La sécurité et la protection des données privées semblent pas encore être pas la priorité des industriels acteurs de ce marché. Les attaques sur les objets connectés présentant des failles de sécurité ont eu tendance à se multiplier ces derniers mois. Caméras de vidéosurveillance, réfrigérateurs, *baby phones*, *Smart TV*, voici quelques exemples connus d'appareils qui ont fait l'objet d'attaques diverses,.

Que faire pour se protéger au mieux contre les attaques ?

La première chose est de lister tous les objets connectés de la maison et de savoir comment et à quoi ils sont connectés (à internet, ou à d'autres objets de la maison). Ensuite, il est impératif de mettre des obstacles sur la route d'un éventuel *hacker*. Pour ce faire, il faut tout d'abord installer régulièrement les mises à jour de sécurité et les mises à jour logicielles, pour limiter le nombre de vulnérabilités connues qui pourraient être exploitées. Il est également nécessaire de changer le nom et le mot de passe par défaut de chaque objet connecté. C'est, en effet, la première chose qu'un *hacker* tentera d'attaquer pour en prendre le contrôle. Pour finir, il convient de limiter l'accès d'un objet connecté aux autres objets connectés dans la maison. Par exemple, si vous avez une *Smart* TV, vous devrez restreindre l'accès à cette TV et autoriser seulement son accès à des ressources particulières du réseau (il n'est pas vraiment nécessaire que votre imprimante soit connectée à votre TV, par exemple, etc.).

La principale faille qu'exploitent les *hackers* est encore trop souvent l'absence de vigilance des utilisateurs. Beaucoup n'ont pas conscience des risques et n'utilisent pas de mots de passe pour protéger l'accès à distance de leurs équipements, ou se contentent de laisser les identifiants par défaut fournis par les fabricants. Un vrai

problème, d'autant qu'avec certains moteurs de recherche spécialisés, tous les appareils connectés ayant une adresse *IP* visible sont désormais répertoriés sur le *Web*.

D'une efficacité redoutable, ce service permet d'effectuer des recherches globales, ou par pays, en saisissant une simple requête pour identifier, localiser, voire prendre le contrôle des appareils connectés non protégés par un mot de passe.

Textes applicables

- Code pénal :
  - Art 313-3 (tentative d'escroquerie)
  - et Art 226-1 (atteinte à la vie privée)

Liens et adresses utiles

- Commission nationale informatique et libertés (CNIL)
- Office central de lutte c/la criminalité et de la communication (OCLCTIC)

Les éléments ci-dessus sont donnés à titre d'information. Ils ne sont pas forcément exhaustifs et ne sauraient se substituer à la réglementation applicable.
Pour tout renseignement complémentaire, reportez-vous aux textes applicables ou rapprochez-vous de la direction départementale de la protection des populations (DDPP) ou de la direction départementale de la cohésion sociale et de la protection des populations (DDCSPP) de votre département.

Actualisation mai 2015