Objets connectés

Lunettes, lave-linge, téléviseurs, montres, systèmes de vidéosurveillance, etc., autant d'objets connectés qui vont peu à peu partager 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 peut ainsi surveiller sa maison à distance et son rythme cardiaque sur l'écran de son « *smartphone* ».

Jusqu'à récemment, ces technologies se limitaient à la sphère professionnelle et pour les particuliers, aux smartphones et ordinateurs portables.

En 2015, les "nouveaux produits connectés" ont représenté un marché de 340 millions d'euros en France en 2015, contre 150 millions en 2014 (marché multiplié par 2,3). Le marché avait déjà doublé entre 2013 et 2014. Les objets connectés représenteraient désormais un peu plus de 2% des ventes de produits électroniques en France en 2015 (institut GfK).
Selon l'institut GfK, la croissance de ces produits n'est cependant pas homogène et varie selon les catégories. Ainsi, 1,22 million de montres et bracelets ont été vendus en France en 2015. En revanche, les objets connectés représentent pour l'instant à peine 1% du chiffre d'affaires de l'électroménager et seulement 5% du marché de la domotique.

Dans une enquête réalisée par l'IFOP[1] en 2015, 23% des français interrogés déclarent posséder au moins un objet connecté : bracelet connecté pour mesurer l'activité ou la condition physique (5%), montre connectée (5%), thermostat connecté (8%), volets roulants (4%), aspirateur (3%), balance connectée (5%), réfrigérateur (2%).

[1] Objets connectés et usage des données - La perception des Français

Cette même enquête montre que la moitié des personnes interrogées se dit effrayée par le risque de fuite des données personnelles, et les deux tiers (68%) considèrent que les données sont mal protégées.

Selon le cabinet d'études économiques Xerfi, la part des objets connectés dans les dépenses high-tech des Français se situait en 2013 autour de 1,5 %, soit 150 millions d'euros. XERFI prévoit une progression régulière de ces dépenses qui pourraient atteindre 500 millions d'euros en 2016.

Une vigilance nécessaire de la part des consommateurs

Le développement 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. Les objets communicants reçoivent, interprètent et communiquent entre eux les données préalablement collectées.

- Les risques de piratage

Dès lors que «se connecter à internet» devient une fonction intégrante d'objets du quotidien les concepteurs de ces équipements doivent faire face aux risques des « *cybers* » attaques.

Que faire pour se protéger?

Dans un premier temps, il convient lors de l'achat de produits dits « connectés » de bien s'informer sur les caractéristiques de ces produits, sur la façon dont ils fonctionnent, sur les interactions, les précautions à prendre le cas échéant.

Pour ce qui est déjà dans la maison, il est possible d'identifier les objets connectés et de rechercher comment ils sont connectés (à internet, ou à d'autres objets de la maison) en vue de mettre en place les outils de protection disponibles : exemple, procéder régulièrement aux mises à jour de sécurité et 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. 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 TV connectée, vous devrez vous assurer de modifier les mots de passe par défaut et choisir un réseau personnel, sécurisé avec une clé de protection adéquate pour le « *wifi* » et le routeur. Même chose pour les mots de passe des services « *web* » et sites internet. Il faudra éviter la redondance des mots de passe entre les différents appareils et sites internet. L'utilisation de mots de passe robustes (mélangeant des majuscules et des minuscules, des chiffres et des caractères spéciaux (%, #, :, $, *), est nécessaire. Leur changement régulier apporte un gain de sécurité supplémentaire. Pour cette TV connectée, restreindre l'accès à votre réseau personnel et isoler son accès à internet des autres éléments connectés au réseau (il n'est pas vraiment nécessaire que votre imprimante soit connectée à votre TV, par exemple, etc.).

La principale faille qu'exploitent les pirates 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.

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 novembre 2016