

FICHES PRATIQUES



Objets connectés : Les risques à connaître

Contrôler sa glycémie sur sa montre, suivre ses performances au golf ou au tennis sur son téléphone, déclencher à distance la climatisation de son domicile... les domaines d'application des objets connectés sont très variés. Mais attention à bien sécuriser les informations qui transitent sur ces appareils !

Qu'est-ce qu'un objet connecté ?

Il s'agit d'un objet qui a la capacité de se connecter à un réseau de communication (Internet des Objets (IDO) via Wi-Fi, Bluetooth, réseau internet mobile notamment 5G...) et peut selon les cas, recevoir, stocker, traiter et transmettre des données, recevoir et donner des instructions pour fonctionner. Ces objets peuvent être autonomes ou fonctionner avec un smartphone ou une tablette permettant de les contrôler ou de servir de relais pour échanger des données.

Ces données peuvent être consultables sur l'appareil mobile ou sur un service Internet.

Un marché en plein essor mais encore hétérogène

L'Internet des objets se développe dans de nombreux secteurs. Il investit progressivement

le marché des applications grand public après s'être développé dans les domaines industriel et professionnel (maintenance d'équipements, gestion de chaînes logistiques...). Le secteur des équipements de la maison connectés s'est particulièrement développé et représente plus de la moitié du chiffre d'affaires issu de la commercialisation des objets connectés, suivi par celui des objets personnels (*wearables*) comme les montres connectées. Au niveau national, les objets connectés grand public ont représenté en 2018 un marché de 1,1 milliard d'euros, dont 55 % pour le secteur de la maison (Smart Home), 31 % pour les objets personnels (*wearables*), 12 % pour les drones et gadgets et 2 % pour les applications liées à la santé.

En termes de parc installé, le bassin parisien concentre 42 % des possesseurs d'objets connectés, tous types confondus. Cela s'explique par une plus grande offre de magasins spécialisés, ou dotés de rayons spécifiques, et

une population plus urbaine à fort pouvoir d'achat.

En 2018, le marché des objets connectés portés – montres, bracelets, lunettes et autres accessoires connectés – a été évalué à 354 millions €, et une large majorité de téléviseurs et de produits Hi-Fi (notamment enceintes et écouteurs avec ou sans réduction de bruit) sont aujourd'hui connectés.

Un niveau d'équipement encore faible

Dans une enquête réalisée par l'IFOP, seulement 22 % des Français interrogés déclaraient posséder au moins un objet connecté : bracelet 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 %).

De même, selon [une étude](#) du cabinet [Xerfi](#) sur le marché des objets connectés, les montres et *trackers* d'activités ne représenteraient que 1 % des dépenses high-tech des Français, loin derrière les smartphones et autres tablettes.

Quels sont les risques ?

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 collectées par ces appareils ;
- le 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.

Comment se protéger ?

- Avant l'achat d'un objet connecté, informez-vous sur ses caractéristiques, son fonctionnement, ses interactions avec les autres appareils électroniques et les dispositifs de protection des données mis en place.

Les domaines d'application

La santé : avec un bracelet, une montre, une balance ou un tensiomètre connecté, il est possible de réaliser des mesures à domicile et de suivre certaines données de santé (comme la fréquence cardiaque, avec certaines montres connectées, qui peuvent d'ailleurs être mises sur marché en tant que dispositifs médicaux), seul ou en collaboration avec un médecin.

Le sport : il est possible de comptabiliser les kilomètres courus ou marchés et synchroniser ces résultats sur un smartphone ou une tablette. Certains appareils, équipés d'un GPS, sont plus particulièrement dédiés aux amateurs de running. Il existe aussi des capteurs pour le golf ou pour le tennis, destinés à mesurer, analyser et améliorer vos performances.

Les loisirs et la vie quotidienne : avec les montres connectées, il est possible de recevoir ses courriels et SMS, accéder à sa musique ou photos et vidéos, calculer un itinéraire, etc. N'oublions pas les téléviseurs connectés qui donnent accès à des contenus multimédias, des applications de loisir ou pratiques, des renseignements sur les programmes regardés, etc.

La domotique et la sécurité : citons, par exemple, les caméras de sécurité, qui permettent de contrôler le domicile à distance et alertent en cas d'intrusion, ou encore les *babyphones*, grâce auxquels il est possible de garder un œil sur les jeunes enfants.

Les économies d'énergie : les objets connectés permettent de connaître, régler et optimiser la consommation énergétique. Par exemple, un thermostat connecté permet de régler à distance la température ambiante, d'optimiser le chauffage en fonction du moment de la journée et du temps de présence, etc.

Depuis le 1^{er} janvier 2022 le vendeur d'un bien comportant des éléments numériques, doit informer les consommateurs de la durée durant laquelle les mises à jour logicielles que le producteur fournit, restent compatibles avec les fonctionnalités du bien.

- Après l'achat, sécurisez bien la connexion aux autres appareils communicants, en procédant régulièrement aux mises à jour de sécurité et mises à jour logicielles. L'idée est de limiter les vulnérabilités connues qui pourraient être exploitées par des personnes ou des organisations malveillantes.

- Autre conseil de bon sens, qui vaut pour la plupart des équipements informatiques : changez fréquemment le nom et le mot de passe par défaut de chaque objet connecté.
- Pour finir, limitez l'accès de l'objet connecté aux autres appareils électroniques ou informatiques. Par exemple, si vous avez une TV connectée, vous devrez vous assurer de modifier le mot 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 et sites internet. Il faut éviter la redondance et utiliser des mots de passe robustes (mélangeant des majuscules et des minuscules, des chiffres et des caractères spéciaux (% , # , \$, *)). N'oubliez pas de restreindre l'accès à votre réseau personnel et d'isoler son accès à internet d'autres éléments connectés au réseau (il n'est pas vraiment nécessaire que votre imprimante soit connectée à votre TV, par exemple).
- Sachez enfin que 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. Vous êtes acteurs de votre sécurité !

- En termes de sécurité pour la santé, le principal risque est la délivrance d'une mesure erronée de la fréquence cardiaque du fait de performances insuffisantes conduisant à un suivi imprécis, voire à la détection d'une arythmie.

Textes de référence

Code pénal - [article 313-3](#) (tentative d'escroquerie)
- et [article 226-1](#) (atteinte à la vie privée)

Liens utiles

[Commission nationale informatique et libertés \(CNIL\)](#)

[Office central de lutte contre la criminalité et de la communication \(OCLCTIC\)](#)

Objets connectés : 5 conseils pour les utiliser en toute sécurité

Avant l'achat :

1 Informez-vous sur les caractéristiques du produit, son fonctionnement, ses interactions avec les autres appareils électroniques et, le cas échéant, sur les précautions à prendre.

Après l'achat :

2 Procédez régulièrement aux mises à jour de sécurité et aux mises à jour logicielles.

3 Changez le nom et le mot de passe par défaut de votre objet connecté.

4 Limitez l'accès de votre appareil aux autres objets connectés.

5 Restez vigilant : vous êtes acteur de votre propre sécurité !

©DGCCRF

Les éléments ci-dessus sont donnés à titre d'information. Ils ne sont pas forcément exhaustifs et ne sauraient se substituer aux textes officiels.

Pour signaler un problème de consommation à une entreprise et se renseigner sur ses droits :



Pour être alerté des produits dangereux :



Pour contacter la DGCCRF :



Pour les personnes sourdes et malentendantes téléchargement de l'application gratuite ACCEO :



Crédit photo : ©Fotolia