Les objets connectés et nous, une relation de confiance ?

Photo Ipopba – Istock

« un projet qui visait à imaginer puis à construire une méthode qualifiante et un banc de tests des objets connectés »

10, 20 ou même 50 milliards d'objets connectés en 2020. Des chiffres qui donnent le tournis mais qui représentent bien plus des espoirs que la réalité car leur déploiement prend plus de temps que prévu. Les utilisateurs potentiels s'interrogent encore sur leur véritable valeur d'usage et nourrissent des doutes sur leur fiabilité. Sont-ils dignes de confiance, tous ces objets connectés qui nous accompagnent dans notre quotidien, au premier rang d'entre eux, le *smartphone*, le couteau suisse du XXIe siècle et le sésame vers l'internet ?

La montée en puissance des objets connectés dans notre vie quotidienne et les soupçons grandissants de mauvais usages des données ainsi connectées à des serveurs peu contrôlables, ont poussé la Fondation MAIF à étudier un banc de test et un label portant sur la confiance apportée à ces objets «communicants».

Jean-Marc Truffet
Responsable Communication et Projets à la fondation MAIF

Un objet connecté, c'est quoi ?

Rien de plus simple : il s'agit d'un objet de tous les jours équipé de capteurs auquel a été jointe une capacité de communiquer. C'est tout simple, mais c'est bien là que tout commence car lorsque le canal de communication s'ouvre, il faut bien le remplir avec des informations. Pour l'utilisateur, ces informations vont augmenter ses capacités, ses connaissances, elles vont le relier à des communautés actives qui partagent les mêmes centres d'intérêt.

Exemples : un robot connecté nous permet d'accéder potentiellement à toutes les recettes du monde et de se séparer du vieux livre de recettes transgénérationnel tout écorné, un bracelet connecté pour la pratique sportive permet d'échanger, de se comparer et de progresser, un compteur de gaz connecté propose d'optimiser sa consommation, une brosse à dents connectée contribue à l'amélioration de l'hygiène bucco-dentaire de son usager, un tensiomètre connecté sécurise son porteur par une surveillance externe et la génération de messages de prévention.

Quels sont les risques liés aux objets connectés ?

Les objets connectés apportent indéniablement une valeur à leurs propriétaires et on peut supposer qu'elle est durable pour celles et ceux qui restent fidèles à leurs acquisitions. Alors pourquoi les objets connectés connaissent-ils un déploiement modéré ?

Plusieurs raisons peuvent l'expliquer : une valeur marchande jugée non proportionnée aux services escomptés, une désaffection d'usage qui vient remplacer l'attrait de la nouveauté et une certaine méfiance quant au mode de fonctionnement de l'objet, notamment vis-à-vis des données personnelles et du respect de la vie privée.

Le manque de transparence des objets ou de l'expertise technique des utilisateurs peut effectivement impliquer des risques que nous pouvons cataloguer ci-dessous, sans chercher l'exhaustivité. Ayons bien conscience que ces risques ne s'appliquent pas systématiquement à tous les objets, les risques dépendent du domaine d'application de l'objet.

Typologie des risques :

- risques de défaillance : le défaut de fonctionnement n'est pas inhérent aux objets connectés. L'incidence de la défaillance dépend alors de l'importance de la fonction de l'objet aux yeux de l'utilisateur (par ex. GPS) ;
- risques de mésusage : l'utilisation incorrecte de l'objet ou l'incompréhension des résultats fournis peut amener un effet contraire à celui escompté (exemple objets connectés liés au sommeil) ;
- risques sur la vie privée : les données collectées par les objets connectés proviennent de notre environnement personnel et décrivent une partie de notre intimité. Ces données peuvent être exploitées à l'insu de l'utilisateur ;
- risques d'intrusion : classiquement, tout objet connecté à Internet est potentiellement vulnérable à des attaques d'intrusion et donc de prise en main par un pirate informatique. Dès lors, l'objet n'obéit plus à son propriétaire légitime. Il peut donc dévoiler ses secrets ou être utilisé comme agent de propagation d'attaques informatiques ;
- risques de blocage de la vie sociale et publique : conséquence du nombre et de l'éventuelle interconnexion des objets entre eux (voiture connectée par exemple), leur infection pourrait provoquer des paralysies sociales.

« une certaine méfiance quant au mode de fonctionnement de l'objet, notamment vis-à-vis des données personnelles et du respect de la vie privée »

Devant ce constat inquiétant, La Fondation Maif a décidé de financer un projet proposé par Digitemis qui visait à imaginer puis à construire une méthode qualifiante et un banc de tests des objets connectés.[1] Digitemis s'est fait une spécialité de combiner la science des ingénieurs en cybersécurité et celle des juristes en termes de protection des données personnelles.

Vers un label de confiance des objets connectés

Le projet s'est rapidement concentré sur la question des données personnelles et du respect du principe de *Privacy by Design*[2] inclus dans le RGPD. Comment faire en sorte que, d'une part, l'acquéreur d'un objet connecté soit correctement informé de l'utilisation de ses données et que son consentement soit systématiquement requis et que, d'autre part, il ait l'assurance de l'absence de « porte dérobée » ? Pour s'assurer qu'un objet connecté respecte bien la législation en vigueur, il faut littéralement le décortiquer et écouter ce qu'il dit.

Exemples de points de contrôle :

- les communications qui sont établies entre l'objet, le terminal de contrôle et les serveurs distants : protocoles utilisés, chiffrement, vulnérabilité ;
- les permissions requises par l'application de contrôle de l'objet sur le terminal de contrôle ;
- les données requises par l'objet : catégories, sécurisation, portabilité ;
- les traitements réalisés sur les données : déclaration, justification, légalité, durée de conservation ;
- les informations dont dispose l'utilisateur : présence, clarté, objectivité.

La recherche a démontré, en auscultant quelques objets connectés typiques, qu'une marge de progrès existe pour atteindre une totale transparence de fonctionnement et une forte résistance aux attaques.

Dans l'optique que ces recherches servent au plus grand nombre, les livrables ont été placés sous licence *Creative Common*[3]. Ils s'adressent en priorité au grand public pour lequel un label qualité a été créé mais aussi aux concepteurs et fabricants d'objets connectés : un guide des bonnes pratiques leur est destiné.

Enfin, la mise à disposition de tous d'un site internet[4] ouvre la voie à une meilleure information des personnes et à une plus grande responsabilisation des acteurs industriels pour une relation de confiance. Reste à convaincre les consommateurs et les producteurs d'objets connectés de l'intérêt d'un dispositif citoyen de ce type, à l'image de l'application *Yuka* dans le domaine de l'alimentation[5]. ■

1. Voir www.fondation-maif.fr/pageArticle.php?rub=1&id=407 et www.digitemis.com
2. « Protection de la vie privée dès la conception », cf. www.cil.cnrs.fr/CIL/spip.php?article2602
3. Droits d'utilisation accordés par des personnes souhaitant libérer leurs œuvres des droits de propriété intellectuelle, à des degrés divers, cf. https://fr.wikipedia.org/wiki/Creative_Commons
4. Cf. www.iotru.st
5. Cf. https://yuka.io