Objets connectés

23 novembre 2021

Que deviennent nos données personnelles ?

Quels risques ?

Dans les domaines du sport, de la santé, de la sécurité, des loisirs, de l'énergie, ils envahissent peu à peu notre quotidien. Les objets connectés sont le plus souvent des smartphones et tablettes, mais peuvent aussi être un robot de cuisine ou un aspirateur, une caméra de sécurité, un compteur électrique, un jouet pour enfant, un téléviseur, une montre, un pèse-personne, un tensiomètre…Ils sont tous équipés d'un matériel électronique qui leur permet de communiquer avec un ordinateur ou un smartphone, ou entre eux, ou vers des serveurs éloignés, via une liaison internet.

Des appli et des pisteurs

Afin de remplir les missions pour lesquelles ils sont fabriqués, ils sont également dotés d'applications qui, elles-mêmes, intègrent des « pisteurs », morceaux de logiciels prévus pour récolter nos données : des données d'usages qui permettent, par exemple, de savoir si l'application fonctionne correctement, mais aussi des données personnelles, certes anonymes, mais associées à un ou des appareils et donc à une personne ou à un foyer. Informés de nos déplacements, de nos achats et paiements, de notre forme physique, de nos goûts culturels, de nos consommations d'énergie, de nos gestes quotidiens, les objets connectés transmettent des milliers de données sur nos modes de vie.

Profilage publicitaire

Ces données, agrégées et monétisées par des sociétés de la AdTech (advertising technologie), définissent notre « profilage publicitaire ». Nos profils, collectivement, valent beaucoup d'argent sur le marché, mais nous, simples

usagers des objets, n'en voyons que le résultat final : les sollicitations publicitaires ciblées déversées constamment sur nos écrans.

Au-delà de la publicité ciblée que les consommateurs subissent, d'autres manipulations de masse, politiques par exemple, sont possibles et se sont déjà produites dans des pays anglo-saxons. Cette surveillance généralisée est appelée par Shoshana Zuboff* « le capitalisme de surveillance ». La sociologue dénonce l'usage commercial qu'une industrie, puissante et opaque, fait de nos données personnelles.

Données consenties

Contre les abus, le Règlement général sur la protection des données (RGPD) est entré en application en Europe en 2018. Il renforce notamment la nécessité du consentement de l'internaute et le droit à l'effacement des données. Comme les internautes donnent généralement leur consentement et qu'il en va souvent du fonctionnement de l'objet ou de certaines de ses applications, le profilage reste une pratique courante. Reste à mettre en place la protection contre un autre risque, le piratage. Dans ce domaine, il est recommandé de changer régulièrement ses mots de passe, de limiter l'accès de l'objet à d'autres objets connectés et de procéder régulièrement aux mises à jour de sécurité et de logiciels.

Michèle Berzosa pour Indecosa-CGT

L'avis d'Indecosa-CGT

L'autorité de la concurrence italienne, il y a deux ans, a jugé que Facebook ne pouvait prétendre fournir un service gratuit puisque l'entreprise utilise les données des internautes dans un but lucratif.

« *Quand c'est gratuit, c'est vous le produit* ». La formule qui daterait des débuts d'Internet reste pertinente aujourd'hui. Le RGPD, la Cnil ou d'autres organismes, se veulent être des parades aux abus mais ces démarches ne sont que des principes de forme qui ne règlent pas le problème de fond : le risque de manipulation des populations à grande échelle par quelques acteurs en situation de monopole. Contre ce risque, les pouvoirs politiques doivent se mobiliser très vite.

Paru dans « Ensemble ! » Journal des syndiqués CGT.

Contacts : indecosa@cgt.fr et indecosa.fr