Les Echos

Vendredi 27 septembre 2019

Pourquoi réguler l'Internet des objets doit être une priorité du législateur

« Les objets connectés destinés au grand public sont aux portes de nos maisons et de notre quotidien. Ils vont nous apporter de réels services mais en contrepartie les risques de détournement et d'utilisation abusive de nos données personnelles n'ont jamais été aussi élevés. » (Par Romuald Cetkovic, dirigeant de 60mn)

Votre bouteille de soda va être connectée ? votre teeshirt ? votre lit ?

Le monde du digital au travers des objets connectés s'immiscera dans quelques mois au cœur de votre domicile et de votre espace de travail. Tous ces capteurs et ces appareils « intelligents »

fonctionneront de façon autonome sans intervention humaine en transférant des volumes de données inédits sur la toile.

Alexa (Amazon), Google home, le compteur électrique Linky ou les luminaires actionnables à distance sont déjà rentrés chez vous. Les premières suspicions sont immédiatement apparues relayées par l'ensemble des médias : écoutes et enregistrements non autorisés, traitements sémantiques utilisés à des fins mercantiles, usurpations d'identité, revente des données collectées.

Mais de nouveaux objets connectés beaucoup plus inoffensifs -en apparence- et surtout beaucoup plus accessibles financièrement se présentent déjà au seuil de votre voiture, chambre ou frigidaire.

Le nombre d'objets connectés va littéralement exploser dans les 5 ans en passant de 15 milliards en 2019 à plus de 25 milliards en 2025.

Etude Garner-Octobre 2018

Que ce soit votre presse agrume, votre réveil ou encore votre bouteille de vin, tous ces objets du quotidien vont se connecter au web pour vous offrir de nouveaux services, pour vous permettre de gagner du temps, de l'argent ou pour vous faciliter la vie au quotidien. Mais ils vont surtout transmettre des données aux industriels et commerçants telles que la composition de votre foyer, la température dans votre salon, votre heure de coucher ou encore votre profil psychologique.

Par exemple, votre machine à café sera capable de vous reconnaitre lorsque vous approcherez et pourra amorcer de façon autonome la préparation d'un café parfaitement adapté à vos goûts en fonction du moment de la journée. Cette même machine pourra vous proposer des recettes sur son écran tactile en façade, pourra vous proposer de visualiser de la publicité ultra segmentée sur ce même écran en contrepartie d'une réduction sur votre prochaine commande de café. Elle gérera bien entendu de façon autonome votre stock de café et les commandes de réassort. Accessoirement elle se bloquera « machinalement » quand vous aurez dépassé les 5 cafés par jour autorisés par votre médecin ou qu'elle aura identifié que votre pression artérielle est trop élevée.

Dès lors que l'on projette l'usage de ces objets connectés à des services liés à notre santé ou à nos opinions personnelles, les premières réticences et interrogations apparaissent.

En premier lieu la connectivité de ces objets au web est très difficilement sécurisable en raison de la complexité et de la diversité des types de transfert entre l'objet connecté et le réseau Internet. Il est donc tout à fait envisageable qu'un individu malveillant récolte vos données ou encore interagisse directement avec l'objet en question afin d'en détourner l'usage. Comme la 5G va contribuer à démultiplier des connexions plus rapides à moindre coût, les cybercriminels se tourneront de plus en plus vers les objets connectés pour arriver à leur fin.

Le second point d'attention est l'obtention des consentements utilisateurs pour le transfert et la collecte de leur donnée. Elle est rendue presque impossible par la nature même de l'objet (par exemple comment lire des conditions d'utilisation de ses données personnelles et valider un consentement explicite via un réveil ?).

De plus, ces objets ne connaissent pas les frontières et donc la collecte de données sensibles en France pourra être utilisée légalement aux USA. Où toutes nos informations personnelles vont-elles être traitées, consolidées et analysées ?

Pour rappel, le "CLOUD Act", adoptée en mars 2018 par le Congrès des Etats-Unis, permet aux autorités américaines de réclamer les données personnelles récoltées par leurs entreprises nationales à l'intérieur comme à l'extérieur des Etats-Unis.

L'exemple du système de crédit social (projet du gouvernement chinois visant à mettre en place un système national de réputation des citoyens) illustre également la porosité des liens entre IoT, business et raison d'Etats puisqu'une grande partie du système repose sur des outils IoT de surveillance de masse.

"Le Cloud Act encourage le dialogue diplomatique mais donne également au secteur de la technologie deux droits statutaires de protéger les consommateurs et de résoudre les conflits de droit s'ils se produisent"

-Lettre commune des principales entreprises NexTEch américaines parmi lesquels Apple, Microsoft, Facebook et Google-

---

Enfin les entreprises sont censées permettre aux utilisateurs d'accéder, utiliser, modifier et supprimer leurs données. Qui plus est, nous sommes également sensés donner notre autorisation explicite pour l'application d'une décision machine (potentiellement négative) ayant un impact sur notre vie privée. Comment mettre en place de place de telles procédures pour les entreprises et comment le consommateur peut-il les assimiler consciemment alors que ces objets du quotidien vont se multiplier autour de nous dans l'avenir ?

C'est pourquoi il est vain de croire que les entreprises arriveront à définir seules un cadre uniforme de bonne conduite. Il est donc indispensable que le législateur définisse les règles du jeu, les obligations et les limites pour tous ces objets connectés.

La priorité doit viser les modalités de cryptage, de transfert et de stockage des données. Ces protocoles doivent être normés et contraints par un cadre juridique solide (avec des menaces de sanctions financières à la hauteur des enjeux) afin de protéger les données privées des citoyens.

La mise en place d'un conseil d'éthique sur ce sujet doit être la seconde priorité des gouvernements. Son rôle ne doit pas se cantonner à être consultatif et nécessite la mise en place d'équipes pluridisciplinaires organisées autour d'une expertise juridique forte mais aussi d'expertise digitale, algorithmiques et de droit privé.

La RGPD mise en place il y a 18 mois est un premier pas qui a le mérite de créer une prise de conscience dans le grand public. Mais il désormais temps d'accélérer le mouvement car pendant que notre législateur avance pas à pas, l'écosystème digitale et le déploiement des objets connectés se fait à grande vitesse.

Romuald CETKOVIC