JURIDIQUE

Des usages au droit des objets connectés

Les objets connectés, dont le nombre progresse de façon exponentielle, posent de nombreux problèmes en termes de régulation et de sécurité. Le point avec Eric Caprioli et Isabelle Cantero, du cabinet Caprioli & Associés.

Les auteurs

Eric A. CAPRIOLI,
Avocat à la Cour, Docteur en droit, Vice-Président du CESIN.

Isabelle CANTERO, ***Juriste senior, Responsable du Pôle Données personnelles et vie privée (Caprioli & Associés, société d'avocats).***

Au vu des publicités pour Noël, nombreux sont ceux, adolescents sages ou adultes à la page, qui vont découvrir au pied du sapin une montre, un bracelet, une balance ou des lunettes ... cadeaux dont la caractéristique commune sera d'être un objet « intelligent » ou « connecté ». Concrètement, pour les bénéficiaires, les pas, les pulsations, les trajets, les variations de poids, la localisation et bien d'autres informations encore pourront être comptabilisés. Sans doute, auront-ils assez vite la surprise de recevoir des publicités associées à l'usage du précieux cadeau... Du côté des professionnels, les innovations se multiplient autour des objets connectés qui collectent et analysent une partie ou l'ensemble des données produites. Par exemple, une puce pourra transmettre les informations concernant l'usure d'un pneu ou d'une pièce aéronautique à l'unité centrale de la voiture ou de l'avion qui pourra ainsi établir un diagnostic fiable de son état à destination de l'utilisateur. Le marché est plus que porteur comme en témoigne l'étude du Gartner (Forecast : The Internet of Things, Worldwide, 2013, par Gartner, Inc.) qui annonce un chiffre d'affaire global de 1 500 milliards d'euros d'ici 2020 soit plus de 20 milliards d'objets connectés en circulation.

L'internet des objets (« IoT ») peut être présenté comme une nouvelle sorte de réseau où des objets hier inertes (ampoule, bracelet, montre, frigo...) sont aujourd'hui connectés à l'internet. Le réseau se développe notamment via l'interaction grandissante entre ces objets *«intelligents»* et les systèmes d'information via les réseaux numériques. Si de nombreuses opportunités « business » sont à saisir, les risques en termes juridiques et de sécurité se multiplient. N'a-t-on pas vu récemment les possibilités de piratage porter sur un pacemaker ou une automobile ?

Quel respect de la vie privée ?

L'identification univoque d'un objet connecté permet de le repérer selon sa localisation. Mais leur utilisation manque encore de transparence, ce qui entraîne des réactions d'inquiétude et de défiance. La mise en place de la traçabilité des objets peut mener, directement ou indirectement, volontairement ou pas, à celle des individus par le traitement de leurs données à caractère personnel. L'internet des objets pénètre la vie quotidienne. Au sujet des étiquettes intelligentes (RFID), la Cnil a considéré qu'elles pouvaient contenir des données à caractère personnel permettant de « profiler » ou de « tracer » les individus et qu'il convenait de respecter certaines règles[1]. Plus récemment, le G29 a formulé des recommandations sur l'internet des objets pour que les acteurs (fabricants, développeurs d'applications, destinataires des données, etc.) se conforment à la réglementation[2]. Ces acteurs devraient recueillir le consentement des utilisateurs et leur permettre de rester maître du partage et du contrôle de leurs données. En tout état de cause, les utilisateurs doivent pouvoir désactiver la connexion de leurs objets. Le G29 recommande également, à l'instar du futur Règlement européen, que les acteurs procèdent, avant la réalisation de toute nouvelle application, à une analyse d'impact sur la vie privée (Privacy Impact Assessments), qu'ils appliquent les principes du Privacy by Design et du Privacy by Default et qu'ils respectent le droit d'opposition des personnes concernées.

En conséquence, la protection de la vie privée doit intégrer ces innovations technologiques, notamment les recoupements et agrégations de données à caractère personnel qui sont échangées par ses objets. De fait, la question de la finalité des traitements de données personnelles est bien au cœur du débat et au vu des législations européennes, par exemple :

---

[1] Communication de M. Lemoine du 10 mars 2005, www.cnil.fr; voir également le dossier complet Internet des objets et RFID : http://www.cnil.fr/dossiers/technologies/internet-des-objets-et-rfid.

[2] Groupe de l'article 29, Doc. WP233, Opinion 8/2014 on the Recent Developements on the Internet of Things, 16 septembre 2014.

comment anticiper le traitement des données pour des finalités ultérieures très différentes voire incompatibles avec la finalité initiale à l'origine de la collecte ? De plus, ces données peuvent être couvertes par le secret médical ou par le secret professionnel : la pratique du Quantified Self[3], entendu comme l'ensemble des activités qui ont pour objet de comparer avec d'autres internautes les variables de son mode de vie (nutrition, exercice physique, sommeil), soulève les craintes de la Cnil en termes d'accessibilité des données, de lieu de stockage, de leur revente éventuelle ou encore de leur utilisation par une tierce personne.

Quelle sécurité pour les informations échangées et conservées ?

L'un des principaux enjeux des objets connectés consiste à s'assurer de la sécurité des données traitées, c'est-à-dire garantir leur confidentialité et leur sécurité. Mais au préalable, l'identification des risques (juridique, conformité, opérationnel) reste une étape incontournable. L'internet des objets introduit de nombreux changements comme la volumétrie et la nature des données, l'interconnexion des réseaux (d'entreprise, inter-entreprises, ...), l'évolution de la supply chain, la géolocalisation des utilisateurs et l'authentification des accès, la complexité d'intégration, les incidences matérielles sur les individus. C'est pourquoi, il est nécessaire d'adapter et de renforcer la sécurité dans les projets jusqu'à leur gouvernance. La sécurité des données (et par là leur fiabilité) s'entend d'un point de vue technique et organisationnel de leur intégrité, de leur disponibilité et de leur confidentialité au sens de la norme ISO 27001. La sécurité doit être intégrée en amont du projet (Security by design)[4]. De la sécurité découlera non seulement la protection de la vie privée des personnes concernées, mais aussi l'interopérabilité.

[1] INHESJ et CIGREF, Sécurité des objets connectés, décembre 2014, v. p.49.
[3] CNIL, Cahier IP n° 2, mai 2014, Le Corps, Nouvel objet connecté. Du « Quantified self » à la M-santé : les nouveaux territoires de la mise en données du monde : www.cnil.fr.

Quelle interopérabilité pour l'interconnexion ?

Actuellement, le plus souvent, seule l'entreprise qui commercialise un objet connecté peut garantir son utilisation puisqu'elle va créer les applications et l'interface permettant à son utilisateur de gérer les données collectées. L'optimisation des données (volume, qualité) passe par le fait de permettre aux objets issus de différents fournisseurs de compiler leurs données, par exemple de les échanger ou les partager. On parle alors d'interopérabilité qui se définit comme la capacité que possède un produit, à fonctionner avec d'autres produits ou systèmes existants ou futurs et ce sans restriction d'accès ou de mise en œuvre. C'est donc par le mécanisme de la normalisation, c'est-à-dire par l'utilisation de standards techniques que l'on va peu à peu voir se développer l'interopérabilité des objets connectés.
Malheureusement, l'abondance de travaux sur le sujet tend à freiner quelque peu sa progression... En effet, on assiste depuis quelques années à des initiatives sur l'internet des objets émanant d'organisations internationales comme l'Union Internationale des Télécoms (recommandations UIT-T Y.2060 et 2061 de juin 2012) et à la création de multiples groupes de travail (W3C, OASIS, GS1, IETF, IEEE P2413 Working Group ou encore l'Open Interconnect Consortium) dont le but affiché est de développer des normes efficaces applicables à tous les acteurs. Toutefois, au-delà des messages publics, il s'agirait plutôt d'une guerre entre les grands opérateurs dont l'objectif est d'imposer leurs propres standard/normes. Toujours est-il que comme pour l'internet classique, la normalisation sera au cœur du développement de l'internet des objets.
Plusieurs grands groupes comme Microsoft (Lab of Things), Google (Physical Web) ou encore La Poste et son Hub pour objets connectés s'intéressent à l'idée de rassembler la gestion d'objets connectés en une seule et même interface. Ici, l'interopérabilité n'est pas totale puisqu'il faudra passer par un tiers pour pouvoir agglomérer et gérer les données issues des différents objets.

Quels droits, quelles responsabilités ?

En principe, le Droit ne reconnaît pas de droit de propriété sur l'information en tant que tel. En revanche, le droit protège les bases de données. Les fabricants d'objets connectés seront tentés de s'aménager techniquement et contractuellement un monopole sur les informations collectées. Dès l'instant où elles auront de telles données en leur possession, ces entreprises pourront ensuite les traiter, les utiliser, les analyser, voire les vendre à d'autres. Si l'on permet à des applications d'agréger toutes les données des IoT, il est sans doute probable que certains utilisateurs ne respecteront pas les conditions contractuelles des fournisseurs (visant à la propriété exclusive des données). L'intérêt pourrait alors être d'établir des relations contractuelles avec les fabricants de chaque objet afin de pérenniser ces transferts d'informations et d'encadrer l'utilisation des données.
Par ailleurs, les acteurs peuvent engager leur responsabilité sur plusieurs fondements : contractuel, responsabilité civile délictuelle (la responsabilité pour faute des articles 1382 et 1383 du code civil), responsabilité du fait des produits défectueux (art. 1386-1 et s. du code civil), garanties des vices cachés (1641 à 1648 du code civil). Juridiquement, on connaît également la responsabilité du fait des choses que l'on a sous sa garde (art. 1384 du code civil). Mais d'autres délits existent, comme la tromperie sur les qualités substantielles du bien (art. L.213-1 du code de la consommation) et la responsabilité du fait de l'obsolescence programmée (art. L. 213-4-1-1 du code de la consommation. Ces délits sont punis de 2 ans de prison et 300 000 euros d'amende ou 5% du CA moyen sur les 3 dernières années. A ces responsabilités, on peut ajouter les recours fondés sur des actions de groupe (ou Class action à la française). A terme, lorsque les IOT seront généralisés, les tribunaux auront à connaître de nombreux litiges en termes de responsabilités, mais aussi du fait de leur complexité technologique et des multiples intervenants pour déterminer le fait générateur du dommage. ■