670

Les enjeux juridiques de l'Internet des objets

C'est une véritable déferlante d'objets connectés qui s'abat désormais sur les consommateurs. Qu'ils concernent les technologies liées à la domotique, aux loisirs ou au bien-être, ces objets dits « intelligents » vont générer dans les années qui viennent une économie sans commune mesure et vont s'accompagner de nouveaux enjeux juridiques, tant pour les utilisateurs que pour les fabricants.

Caroline Laverdet, avocat à la Cour

Caroline Laverdet interviendra lors de la conférence du 12 juin 2014 : « Les objets connectés - Vers un nouvel environnement juridique ? », organisé par le CEJEM.

Qu'est-ce qu'un objet connecté ?
Jumelés à un smartphone ou reliés à un réseau sans fil, les objets connectés proposent aux consommateurs des services dédiés en traitant des informations de toute nature collectées au moyen de capteurs. Conçus pour interagir entre eux ou simplement analyser les habitudes de leur propriétaire, les objets connectés peuvent prendre la forme d'objets du quotidien ou de *wearable technologies* portées par l'utilisateur, à l'image des lunettes *Google Glass* ou des montres connectées. Toutefois le fonctionnement de ces objets repose nécessairement sur l'exploitation des données personnelles des personnes concernées. De nature très variée, ces données sont collectées en continu auprès du consommateur et transmises dans un volume massif aux responsables de traitement. La technologie des objets connectés s'inscrit donc dans le phénomène *Big Data*, qui se réfère aux outils permettant le traitement et l'analyse rapide d'ensembles volumineux de données. La révolution des objets connectés repose donc sur la valorisation économique des données produites et transmises par les utilisateurs, ces dernières permettant notamment d'alimenter des bases de données à des fins de profilage ou de ciblage publicitaire.

La conclusion de contrats par ou *via* des objets connectés est-elle possible ?
Au-delà des technologies destinées à analyser les habitudes du consommateur, certains objets connectés pourront suppléer voire remplacer l'individu pour effectuer des achats. Les réfrigérateurs connectés sont par exemple capables de lister les denrées qu'ils contiennent et de proposer de passer automatiquement commande lors de l'épuisement des produits. Dans ce contexte, la question se pose de savoir si l'objet connecté conclut lui-même un contrat avec un prestataire, sur ordre de son propriétaire, ou si cet objet n'est qu'un moyen de transmission du consentement de la personne et de son ordre de paiement. Cette dernière thèse semble la plus adaptée au regard des règles de capacité relatives à la formation des contrats, dès lors que l'objet connecté n'est à ce jour doté d'aucun statut juridique. En tant que chose, il ne pourra pas non plus être considéré comme un mandataire, l'article 1984 du Code civil définissant le mandat comme un « *acte par lequel une personne donne à une autre le pouvoir de faire quelque chose pour le mandant et en son nom* ». La commande ne pourra qu'être passée directement par le consommateur au prestataire, qui devra pour sa part respecter les obligations légales en matière de vente en ligne, l'objet connecté devant alors s'analyser comme un moyen de communication. À ce titre, la loi n° 2014-344 du 17 mars 2014 relative à la consommation (V. *JCP G 2014, doctr. 634, Étude J. Bigot, en matière de contrat d'assurance*) qui entrera en vigueur le 14 juin prochain impose notamment l'envoi d'une confirmation de la commande, la mention des caractéristiques du produit et son prix, les délais de livraison. Toutefois, l'abonnement constituera sans nul doute le cadre le plus efficace si le consommateur décide d'être livré d'une liste d'achats prédéfinis à intervalles réguliers.

« Il appartiendra au consommateur de vérifier auprès de son assureur la prise en charge des sinistres causés par des objets connectés. »

Quelle responsabilité en cas de défaillance de l'objet connecté ?
Les ampoules, cafetières, télévisions et autres thermostats connectés offrent à l'utilisateur un contrôle à distance de leur habitat, le plus souvent *via* une application *smartphone*. Or nul n'est à l'abri d'une erreur commise par l'objet connecté lors de la transmission de l'instruction, ou d'une défaillance dans la connexion de l'objet au réseau. L'activation manuelle des fonctions des objets devra donc être prévue, pour permettre par exemple à l'utilisateur d'une serrure connectée de déverrouiller la porte de sa maison en cas de coupure de courant. L'objet connecté étant intelligent, on pourrait également imaginer qu'il constate sa propre défaillance et contacte automatiquement le service après-vente. Les fabricants auront évidemment à cœur de limiter leur responsabilité dans les conditions générales d'utilisation, notamment en cas de force majeure ou du fait de l'intervention d'un tiers. Les accidents de la circulation impliquant des véhicules à conduite automatisée, tels que les *Google Cars*, soulèveront toutefois de véritables problématiques de responsabilité du fait des choses. Une adaptation de la législation relative à ce moyen de transport connecté, dès lors qu'il ne requiert pas de pilote, devra être envisagée avant d'autoriser leur déploiement. Enfin, il appartiendra au consommateur de vérifier auprès de son assureur la prise en charge des sinistres causés par des objets connectés, où d'adhérer à une assurance particulière.

Quelles sont les données concernées par le *quantified self* ?
Ce phénomène d'auto-évaluation des habitudes de vie est aujourd'hui amplifié par la mise en circulation de montres podomètres, brosses à dents et autres objets connectés mesurant les données corporelles relatives au bien-être de l'individu. Or ces informations peuvent facilement s'apparenter à des données de santé, définies par l'article 4 du projet de Règlement européen sur

la protection des données personnelles (*COM(2012) 11 final, 25 janv. 2012*) comme « *toute information relative à la santé physique ou mentale d'une personne, ou à la prestation de services de santé à cette personne* » et soumises à un régime juridique particulier. Elles constituent en effet des données sensibles dont le traitement et la collecte sont par principe interdits par la loi Informatique et libertés, à moins que la personne concernée n'ait donné son consentement exprès. L'article L.1111-8 du Code de la santé publique impose également à l'hébergeur de données de santé l'obtention d'un agrément préalable du ministre chargé de la Santé. Le fabriquant d'un objet connecté qui héberge, analyse et renvoie des données de bien-être au consommateur pourrait donc se voir imposer les obligations relatives aux données de santé si les caractéristiques de ces deux types de données ne sont pas rapidement clarifiées.

Quelles obligations relatives à la sécurité des objets connectés ?

Du fait de leur connexion à un réseau, les risques de piratage des objets connectés sont réels. En cas de vol ou d'intrusion dans le terminal mobile contrôlant les objets connectés d'une maison, les alarmes, serrures et coffres-forts seront alors déverrouillés et accessibles aux cambrioleurs. Au vu de telles menaces, l'article 34 de la loi Informatique et libertés (*L. n° 78-17, 6 janv. 1978*) impose au responsable du traitement des données « *de prendre toutes précautions utiles (…) pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès* ». Le non-respect de ces dispositions est puni par l'article 226-17 du Code pénal de cinq ans d'emprisonnement et de 300 000 euros d'amende, celle-ci pouvant atteindre 1 500 000 euros pour les personnes morales. Toutefois le caractère dissuasif de ces sanctions peut être discuté, au regard du volume de données personnelles en jeu. Concernant les moyens concrets de sécurisation des objets connectés, les experts en sécurité informatique misent notamment sur la protection de chaque objet par mot de passe, leur authentification *via* des certificats, la mise en œuvre d'une politique transparente de confidentialité et d'archivage des données, le déploiement rapide des corrections de failles de sécurité et l'incitation des consommateurs à prendre conscience de la nécessité de protéger leurs données personnelles.

Quel impact aura le projet de règlement européen relatif aux données personnelles sur les objets connectés ?

La proposition de règlement sur la protection des données en date du 25 janvier 2012 a pour objectif de redéfinir le cadre juridique établi par la directive 95/46/CE du 24 octobre 1995, en prenant en compte le développement des nouvelles technologies depuis ces vingt dernières années. Les responsables de traitements auront désormais une obligation d'*accountability*, qui leur imposera d'adopter des procédures particulières pour garantir et justifier du respect des dispositions légales en matière de protection des données personnelles. Pour assurer la mise en œuvre de ces principes de protection, sont notamment prévues des obligations de « documentation » (*Prop., art. 28*), d'analyses d'impact de certains traitements à risques, également appelées *Privacy Impact Assessment* (ou analyse d'impact relative à la protection des données : *Prop., art. 33*), et d'intégration de mécanismes de protection des données personnelles dès la conception de l'objet en application des notions de *privacy by design* et de *privacy by default* (ou protection des données dès la conception et protection des données par défaut : *Prop., art. 23*). Par ailleurs, les entreprises de plus de 250 salariés devront désigner un délégué à la protection des données (*Prop., art. 35*), lequel devra désormais contrôler que le responsable de traitement respecte l'ensemble de ses obligations, et non plus seulement s'assurer de la conformité à la loi Informatique et Libertés. Enfin, les autorités nationales de protection des données pourront prononcer des sanctions financières allant jusqu'à 2 % du chiffre d'affaires d'une entreprise. La technologie des objets connectés reposant en grande partie sur le traitement massif de données personnelles, les fabricants doivent donc se préparer à respecter les exigences du projet de règlement européen.

Un droit à la désactivation des puces peut-il être envisagé ?

La plupart des objets connectés peuvent communiquer avec d'autres appareils et sont de ce fait équipés de puces RFID ou de systèmes analogues leur permettant de se reconnaître entre eux. C'est donc plusieurs fabricants potentiels d'objets connectés qui pourront avoir accès aux données des consommateurs. Face à ce risque d'intrusion dont l'individu n'aura pas forcément été clairement informé, l'hypothèse de la désactivation de la connexion de l'appareil et du partage des données doit être envisagée. Ce « droit au silence des puces », préconisé par la Commission européenne dans une recommandation du 12 mai 2009 (*JOUE n° L 122, 16 mai 2009, p. 47*), aurait pour finalité de rendre à l'utilisateur la maîtrise du partage de ses informations, en revenant à une utilisation « normale » de l'objet sans interaction électronique. À l'heure actuelle, dès lors que les puces permettent l'identification directe ou indirecte d'une personne, la loi Informatique et Libertés a vocation à s'appliquer. Ainsi, en fonction de la finalité de la puce installée dans l'objet connecté, la personne concernée doit pouvoir exiger la désactivation de celle-ci sans frais. L'intégration de cette fonctionnalité devra donc être prévue par les fabricants au stade même de la conception de l'objet.

Quel cadre éthique pour les objets connectés ?

Alors que l'Internet des objets promet d'entailler largement la sphère de la vie privée, le marketing des objets connectés se devra de respecter certaines valeurs éthiques pour obtenir et conserver la confiance du consommateur dans les technologies commercialisées. Les objets connectés peuvent en effet adresser à leur propriétaire des notifications sur l'écran du smartphone, par sms, téléphone, mail, alerte sonore, etc. Ainsi, en matière de publicité, les stratégies commerciales des industriels et des responsables de traitements devront se montrer pertinentes quant aux données collectées mais également respecter un tant soit peu l'intimité de la personne. Certaines compagnies d'assurance analysent déjà les habitudes de leurs assurés et leur proposent des offres tarifaires particulières selon la qualité de leur santé ou de leur mode de vie. En matière de *quantified self*, les utilisateurs de pèse-personnes connectés n'apprécieront pas toujours de se voir proposer des produits amaigrissants. Les règles éthiques dans le traitement des données collectées par les objets connectés seront par nature amenées à évoluer en fonction de la sensibilité des consommateurs, mais leur définition ne sera pas… une mince affaire. ■

> « En matière de *quantified self*, les utilisateurs de pèse-personnes connectés n'apprécieront pas toujours de se voir proposer des produits amaigrissants. »

Bibliographie

L. Marino, L'*open data*, une mine d'or pour les juristes : JCP G 2014, prat. 438

L. Marino, Notre vie privée : des *little* data aux *big data* : JCP G 2012, supplément au n° 47, p. 14

Institut G9+, Livre blanc, Les nouveaux eldorados de l'économie connectée, déc. 2013 : http://www.g9plus.org/interface/2013-12-G9plus-NouveauxEldorados.pdf

C. Laverdet, Données personnelles : bilan de 1995 et réforme de 2014 ? Compte-rendu du colloque du CEJEM du 20 mars 2014 : RLDI janv. 2014, n° 3181