ADAMAS
Avocats associés

lyon paris
pékin shanghai

L'INTERNET DES OBJETS ET L'ECHEVEAU JURIDIQUE D'UN MONDE PLUS CONNECTE

Selon la Commission européenne, l'internet des objets se compose d'une « *série de nouveaux systèmes indépendants fonctionnant avec leurs propres infrastructures qui reposent en partie sur les infrastructures existantes de l'internet* »[1].

Lunettes de réalité augmentée, montres cardio/podométriques et autres traqueurs d'activité, dispositifs médicaux connectés, systèmes domotiques de sécurité et de confort de la maison, objets intelligents de gestion de l'énergie, miroirs interactifs et réfrigérateurs contrôlant notre consommation alimentaire, … Les objets connectés envahissent notre quotidien et leurs applications sont multiples.

D'aucuns estiment qu'il y aura 25 milliards d'objets connectés à internet dans le monde en 2015 et 50 milliards en 2020[2].

Avec des start-up innovantes comme, par exemple, la société Bioserenity et ses vêtements connectés ou encore la société Withings et ses objets de bien-être et santé connectés, la France saura sans doute exploiter son savoir-faire et tirer profit de ces perspectives. Le marché français des objets connectés aurait déjà pesé 150 millions d'euros en 2013 et devrait représenter 500 millions d'euros en 2016[3], alors même qu'il n'exprimera pas encore toutes ses potentialités, pour des raisons qu'il n'est pas utile de présenter ici.

Toutes ces nouvelles technologies vont bouleverser en profondeur les interactions entre les hommes et les objets et, en définitive, les rapports entre les hommes. Naturellement, ceci soulèvera de nombreuses problématiques juridiques complexes et autant de défis nouveaux pour les juristes.

Le cadre juridique de l'internet des objets est, en effet, hétéroclite et emprunte à divers domaines juridiques (droit des contrats, droit de la responsabilité, protection des données personnelles, droit de la propriété intellectuelle,…).

L'un des problèmes juridiques principaux, qui est apparu d'emblée, est sans aucun doute celui de la protection de la vie privée et des données à caractère personnel.

[1] « *L'internet des objets : un plan d'action pour l'Europe* » Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions en date du 18 juin 2009 (COM/2009/0278 final)
[2] "*The Internet of Things. How the next evolution of the internet is changing everything*", Dave Evans, CISCO IBSG, Avril 2011
[3] http://www.journaldunet.com/ebusiness/le-net/marche-objets-connectes-selon-xerfi.shtml

e-mail
infocom@adamas-lawfirm.com

www.adamas-lawfirm.com

lyon paris
pékin shanghai

Diverses organisations étatiques et supra-étatiques se sont d'ailleurs rapidement penchées sur la question, dont notamment la « Federal Trade Commission » américaine[4] ou la Commission européenne[5].

Récemment, le Groupe de travail « Article 29 », regroupant les autorités de protection des données personnelles européennes, a adopté un avis relatif aux « Récents développements de l'internet des objets »[6]. L'objectif du G29 est de contribuer à l'uniformisation du cadre juridique européen de la protection des données à caractère personnel et au développement d'un haut niveau de protection de celles-ci dans le contexte des objets connectés.

Dans cet avis, rendu le 16 septembre 2014, le G29 s'est focalisé sur trois catégories d'objets connectés : les dispositifs portables (« *Wearable Computing* », comme par exemple les lunettes et montres connectées), les dispositifs de mesure de soi (« *Quantified Self* », comme par exemple les moniteurs de santé) et les appareils domotiques (« *Home Automation* »). Le G29 a identifié les principaux problèmes liés à la protection des données personnelles résultant des objets connectés, et en particulier 1) l'absence de contrôle de l'utilisateur sur la diffusion de ses données, 2) le consentement éclairé de l'utilisateur, 3) la réorientation de la finalité d'origine du traitement de données, 4) le profilage intrusif et l'analyse comportementale, 5) les difficultés pour assurer l'anonymat et, enfin, 6) les difficultés d'assurer un équilibre entre la sécurité des données et des objets connectés et leur efficacité technique.

Le G29 a ensuite proposé une série de recommandations pratiques communes puis spécifiques aux principaux acteurs du secteur, afin qu'ils puissent développer un écosystème durable de l'internet des objets tout en respectant la législation en vigueur. A titre d'exemples, le G29 a recommandé la mise en place d'études d'impact préalablement à tout lancement de nouvelles applications dans l'internet des objets[7], l'agrégation des données, l'application des principes de protection des données dès la conception (« *Privacy by design* »)[8] et par défaut (« *Privacy by default* »)[9] ou encore la possibilité pour l'utilisateur de demeurer maître de ses données personnelles à tout moment (principe de « *self-determination* »).

Concernant plus particulièrement les traitements de données par les objets connectés, ainsi que l'a soulevé le G29 dans son avis du 16 septembre 2014, de nombreux

[4] V. par ex. "*The Internet of Things: From Regulators, Guidance and Enforcement*", New York Times, 8 septembre 2013.
[5] « *L'internet des objets : un plan d'action pour l'Europe* » Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions en date du 18 juin 2009 (COM/2009/0278 final)
[6] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf
[7] Les études d'impact sur la vie privée des traitements de données personnelles font notamment partie des mesures préventives de détection et de gestion d'incidents de sécurité que la Commission européenne, dans la proposition de Règlement européen de protection des personnes physiques à l'égard du traitement des données à caractère personnel, adopté en 1ère et unique lecture, le 12 mars 2014, envisage de rendre obligatoires.
Lien vers le texte de la proposition de Règlement : http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0212+0+DOC+XML+V0//FR
[8] Ce concept, élaboré dans les années 90, consiste à assurer la protection de la vie privée en l'intégrant dès la conception et tout au long du processus de réalisation des technologies.
[9] Ces principes sont également repris dans la proposition de Règlement européen adoptée en mars 2014, à l'Amendement 118. Le paragraphe 2 définit le principe de protection des données par défaut ainsi : « *Le responsable du traitement s'assure que, par défaut, seules seront traitées les données à caractère personnel nécessaires à chaque finalité spécifique du traitement, ces données n'étant, en particulier, pas collectées, conservées ou communiquées au-delà du minimum nécessaire à ces finalités, pour ce qui est tant de la quantité de données que de la durée de leur conservation. En particulier, ces mécanismes garantissent que, par défaut, les données à caractère personnel ne sont pas rendues accessibles à un nombre indéterminé de personnes physiques et que les personnes concernées ont la possibilité de contrôler la diffusion de leurs données à caractère personnel.* »

e-mail
infocom@adamas-lawfirm.com

www.adamas-lawfirm.com

lyon paris
pékin shanghai

intervenants dans la chaîne de conception de ces objets peuvent avoir accès aux données des utilisateurs. Pour garantir les droits de ces derniers, des procédures devraient donc être mises en place entre ces intervenants, afin de faire remonter les demandes des utilisateurs quant à leurs données personnelles (droits à l'information, d'accès, de rectification, d'opposition, d'interopérabilité, de retrait). A cette fin, il semble nécessaire, en premier lieu, de définir et délimiter précisément les rôles et obligations de chaque intervenant (responsable du traitement, sous-traitant, destinataire des données). Les droits des intervenants quant à l'utilisation des données devraient également être clarifiés, en particulier au regard de la finalité du traitement, qui doit être définie avant toute collecte des données et impose, en conséquence, à l'ensemble des acteurs d'avoir très en amont une vue globale du projet envisagé.

Les objets connectés soulèvent, enfin, des problématiques de sécurité et de confidentialité des données, en particulier lorsqu'il s'agit de données de santé[10]. Il est impératif d'évaluer, très en amont, les risques liés aux réseaux de communication sur lesquels les données vont circuler, les risques liés à la sécurité (*phishing*, usurpation d'identité, *spamming,* prise de contrôle à distance, …) et à la confidentialité des données (échanges, partages, transferts, regroupement de données, connexions intempestives entre les objets, …).

L'internet des objets soulève donc des problèmes complexes en matière de vie privée et de protection des données personnelles. Mais cela est également le cas en matière de responsabilité, de propriété intellectuelle,… L'internet des objets s'inscrit dans un écheveau juridique dont la complexité apparait progressivement mais moins vite que la fulgurante progression des technologies connectées. Il n'en demeure pas moins nécessaire de penser et d'établir les solutions juridiques qui protègeront les utilisateurs et sécuriseront les opérateurs, sans quoi l'écosystème des objets connectés et le progrès technologique qu'il génère pourront être freinés.

Jean-Baptiste CHANIAL
Avocat Associé

Lucille ROMESTIN
Avocat

[10] Les objets connectés de santé de type « *quantified self* » reposent sur la collecte de données *a priori* non sensibles (rythme cardiaque, poids, etc.) mais qui cumulées peuvent créer un fichier clinique de la personne et donc constituer de véritables données de santé. Ces dernières profitant d'une protection renforcée, un traitement spécifique doit leur être réservé afin de préserver la confidentialité des données et le respect de la vie privée des utilisateurs.

e-mail
infocom@adamas-lawfirm.com

www.adamas-lawfirm.com