JTIT Internationale n°6 – fév. 2014
Special international issue #6 – Feb. 2014
ALAIN BENSOUSSAN
Juristendances Informatique et Télécoms
Le réseau Lexing® vous informe – The Lexing® network informs

L'INTERNET DES OBJETS

INTERNET OF THINGS

L'Internet des objets : aspects légaux

▪ L'internet des objets n'est plus un sujet futuriste. Aujourd'hui, on considère qu'une personne est en moyenne connectée à deux outils ou applications.

▪ Plutôt que de parler de l'Internet des objets, on doit d'ailleurs parler d'objets connectés ou d' « objets intelligents ».

▪ Evidemment, ces nouveaux usages posent d'innombrables questions juridiques.

▪ Le problème est que pour une question transnationale, les réponses restent à ce stade nationales.

Les membres du réseau Lexing® dressent un tableau de la situation actuelle à travers le monde.

Internet of Things: legal aspects

▪ *The Internet of Things is no longer a futuristic topic. Today, an average person has at least two objects or applications connected to the Internet.*

▪ *Rather than talking of the Internet of things, it would be more adequate to refer to "connected things" or "smart things".*

▪ *And these new things clearly raise a string of legal issues.*

▪ *The problem is that while it is a transnational issue, the fact remains that, to date, solutions are primarily provided at the national level.*

The Lexing® network members provide a snapshot of the current state of play worldwide.

A propos de Lexing®

Lexing® est le premier réseau international d'avocats technologues dédié au droit des technologies avancées.

Créé sur une initiative d'Alain Bensoussan, Lexing® permet aux entreprises internationales de bénéficier de l'assistance d'avocats alliant la connaissance des technologies, des métiers et du droit qui leur sont applicables dans leur pays respectifs.

About Lexing®

Lexing® is the first international network of lawyers dedicated to technology law.

Created on an initiative of Alain Bensoussan, Lexing® allows multinationals to benefit from the assistance of seasoned lawyers worldwide who each combines unique expertise in technology and industry with a thorough knowledge of law in their respective country.

ERIC BARBRY

L'IdO, la protection des données et les nouvelles technologies au Royaume-Uni

▪ L'Internet des objets ayant vocation à combiner toutes sortes de communications, partout, tout le temps, pour tout le monde, et sur n'importe quel support, quel que soit le contenu, il est légitime de s'interroger sur la capacité de la réglementation britannique en matière de protection des données à faire face aux nouvelles technologies mises en œuvre dans le cadre de l'IdO, et notamment la RFID (identification par radiofréquence). La RFID est une technologie repose sur l'utilisation d'un couplage électromagnétique ou électrostatique dans le spectre radioélectrique qui permet d'identifier de façon unique un objet, un animal ou encore une personne. De minuscules puces électroniques (appelées radio-étiquettes, étiquettes ou « tags » RFID) **(1)** peuvent ainsi recevoir et transmettre des informations par ondes radio et identifier une chose ou une personne sans qu'un contact direct préalable soit nécessaire.

▪ En pratique, lorsqu'un lecteur (émetteur-récepteur) RFID entre dans la portée d'une étiquette RFID, celui-ci envoie une requête à l'étiquette, qui lui transmet en retour son code d'identification unique. Au Royaume-Uni, l'utilisation du spectre radio est normalement subordonnée à l'obtention d'une licence octroyée par l'Ofcom **(2)**, l'autorité régulatrice des télécommunications, en vertu de la loi de 2006 sur la télégraphie sans fil **(3)**. Cependant, l'Ofcom a adopté deux textes exemptant de licence certains équipements RFID : l'un en 2005 **(4)** et l'autre en 2007 **(5)**, ce dernier venant élargir encore davantage le premier, à la suite de la décision 2006/804/CE de la Commission européenne relative à l'harmonisation du spectre radioélectrique pour les dispositifs d'identification par radiofréquence (RFID) **(6)**, en supprimant un certain nombre de limitations imposées aux dérogations accordées en 2005.

▪ La technologie RFID est exploitée dans tous les secteurs pour des usages multiples : dans les grands magasins (pour lire les prix des produits au passage en caisse), dans les entrepôts (pour procéder à l'inventaire des stocks), pour les zones sécurisées (dont l'accès est soumis à l'utilisation d'une carte à puce). Dès lors, des abus et des dérives sont bien entendu possibles. Par exemple, un commerçant peut exploiter les étiquettes RFID apposées sur ses produits en vue de localiser le consommateur après que celui-ci a quitté son magasin, récoltant de cette manière de précieuses données marketing. Un des dangers réside donc dans la tentation d'utiliser ces données sans le consentement des personnes concernées à des fins de prospection commerciale, notamment.

▪ Les données ainsi collectées peuvent constituer des « données à caractère personnel » au sens de la loi britannique de 1998 sur la protection des données **(7)**, soit en elles-mêmes, soit du fait de leur combinaison avec d'autres informations (issues des cartes bancaires, des cartes de fidélité etc.) rendant possible l'identification des personnes concernées (et notamment l'acheteur d'un produit incorporant un tag RFID). En outre, si ces données permettent au responsable du traitement de distinguer une personne concernée d'une autre personne concernée, la loi britannique sur la protection des données est susceptible de s'appliquer, quand bien même le responsable du traitement ne serait pas mesure de relier les données RFID à un nom ou une adresse.

▪ L'utilisation de la technologie RFID dans le but d'assurer la gestion de la chaîne d'approvisionnement peut être justifiée lorsque la finalité poursuivie est la protection des intérêts légitimes du responsable du traitement. Pour toutes autres finalités (prospection commerciale, par exemple), le moyen le plus sûr de s'assurer de la conformité légale du traitement des données mis en œuvre est d'obtenir le consentement de la personne concernée, en affichant, de manière claire, des mentions d'informations à côté des produits incorporant des tags RFID ou directement sur ceux-ci, en indiquant les raisons pour lesquelles les données collectées seront utilisées. Dans le cas où un commerçant souhaite géolocaliser le produit, il conviendrait de préciser cette finalité au sein de la mention d'information, d'autant plus que cette précision serait nécessaire pour garantir un traitement loyal des données.

▪ Dès septembre 2006, l'autorité britannique de protection des données, l'ICO **(8)**, a publié une note d'orientation technique à l'usage des utilisateurs de la technologie RFID **(9)**. Partant du constat du recours croissant à la RFID, l'ICO a estimé nécessaire de préciser dans une note les conditions dans lesquelles elle pouvait être utilisée dans le respect de la loi sur la protection des données. Cette note souligne qu'il incombe aux personnes qui collectent des données personnelles au moyen de radio-étiquettes d'effectuer les actions suivantes :

- Informer les personnes concernées que leurs produits comportent des étiquettes RFID et leur expliquer quelles informations sont collectées, par qui et dans quel but ;
- Utiliser des mots de passe et des moyens de cryptage permettant de lutter contre le « slamming » (détournement ou captation des tags RFID par des dispositifs de lecture non autorisés) et le « cloning » (copie non autorisée de données personnelles à partir de tags RFID, en vue notamment d'usurper une identité) ;
- Limiter l'utilisation des données à caractère personnel en résultant à des finalités légitimes déterminées dans le respect des autres principes de protection des données ;
- Gérer ces questions à un stade précoce, c'est-à-dire en amont, lors dès la conception de l'architecture du système RFID.

▪ En conclusion, si les développements technologiques futurs pourraient nécessiter une modification de la législation britannique sur la protection des données, pour l'heure, il semble que la RFID puisse encore être réglementée efficacement par les dispositions actuellement en vigueur au Royaume-Uni.

DANNY PREISKEL

REFERENCES

(1) Wikipédia, page « Radio-identification », http://fr.wikipedia.org/wiki/Radio-identification

(2) Office of Communications (« OFCOM »), http://www.ofcom.org.uk/

(3) Wireless Telegraphy Act 2006, http://www.legislation.gov.uk/ukpga/2006/36/pdfs/ukpga_20060036_en.pdf

(4) Wireless Telegraphy (Radio Frequency Identification Equipment) (Exemption) Regulations 2005 (SI 2005/3471) (2005 Regulations), http://www.legislation.gov.uk/uksi/2005/3471/pdfs/uksi_20053471_en.pdf

(5) Wireless Telegraphy (Radio Frequency Identification Equipment (Exemption) (Amendment) Regulations 2007 (SI 2007/1282) http://www.legislation.gov.uk/uksi/2007/1282/pdfs/uksi_20071282_en.pdf

(6) Décision 2006/804/CE, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:329:0064:0066:FR:PDF

(7) Data Protection Act 1998 http://www.legislation.gov.uk/ukpga/1998/29/data.pdf

(8) Information Commissioner's Office (ICO), www.ico.org.uk

(9) ICO's Data Protection Technical Guidance - Radio Frequency Identification, 09.08.06.

Internet of Things, Data Protection and New Technologies under UK Law

▪ *Since the Internet of things combines communications "anytime, anywhere" for anyone (on any device) with "anything", one might be forgiven for immediately asking how current UK data protection regulations may cope with these new technologies such as for example radio frequency identification (RFID). RFID is a technology that incorporates the use of electromagnetic or electrostatic coupling in the radio frequency spectrum to uniquely identify an object, animal, or person. Tiny microchips (RFID tags) **(1)** which can receive and transmit information by radio waves may therefore allow for identification without any previous direct contact.*

▪ *When an electronic reading device comes within range of the RFID tag, the tag receives a radio query from the reader and it responds by transmitting its unique identification code to the reader. In the UK, any use of the radio spectrum is generally subject to a licence granted by Ofcom under the Wireless Telegraphy Act 2006 **(2)**. However, in December 2005, Ofcom **(3)** adopted the Wireless Telegraphy (Radio Frequency Identification Equipment) (Exemption) Regulations 2005 (SI 2005/3471) (2005 Regulations) **(4)**, which made certain RFID equipment exempt from the licensing requirement and in 2007, following the adoption by the European Commission of Decision 2006/804/EC **(5)** on harmonisation of the radio spectrum for radio frequency identification (RFID) devices, Ofcom adopted a new statutory instrument, the Wireless Telegraphy (Radio Frequency Identification Equipment (Exemption) (Amendment) Regulations 2007 (SI 2007/1282) **(6)**, which removed a number of limitations on the exclusion conferred by the 2005 Regulations.*

▪ *The RFID technology predominately used for retail check-outs (to read product and pricing information), in warehouses (for taking stock inventories) or for security systems (which require people to use smart-cards to gain access to secure areas), however, may also be misused. Considering the common practice in retail, for example, the RFID tags of the products may be used to track the location of the consumer (even after the consumer has left the shop) thereby gaining valuable marketing data. The danger lies in the temptation for retailers to use such data without consent for direct marketing purposes.*

▪ *Any data so collected about individuals may constitute "personal data" as defined in the UK Data Protection Act 1998 ("DPA") **(7)**, on its own, or combined with other information such as credit or loyalty card information so as to enable the individuals concerned (such as the buyer of a product to which the tag is attached) to be identified. Also, if it enables the data controller to distinguish one data subject from another, the DPA may even apply if the data controller is not able to link the RFID data with a name or address.*

▪ *Whereas the use of RFID technology to manage the supply chain may be justified under the DPA because it protects the legitimate interests of the data controller, the safest route to compliance in respect of other uses of data so collected (e.g. direct marketing) would be to gain the consent of the data subject by displaying clear notices next to, or on, the products which contain the tags stating the purposes for which the data will be used. If it is the retailer's intention to track the location of the product, it is probably advisable to state this in the notice as it could be classified as information which is necessary to make the processing fair.*

▪ *In September 2006, the UK Information Commissioner **(8)** published a technical guidance note for those who use RFID technology **(9)**, giving some background about the increasing prevalence of RFID tags and the way in which the DPA governs their use. It emphasises that those who collect personal data using RFID tags must:*

- *Tell data subjects that their products carry RFID tags and must explain what information is collected, by whom and for what purpose.*
- *Use passwords and encryption against "slamming" (the reading of tags by unauthorised reading equipment) and "cloning" (the unauthorised copying of personal data from tags, which can be used for identity theft).*
- *Limit the use of the resulting personal data to specified legitimate purposes and comply with the other data protection principles.*
- *Take account of these issues at an early stage, that is when planning the architecture of the RFID system.*

▪ *Although future developments may require an amendment of UK data protection legislation, it seems as if RFID technology may still be regulated successfully by the current provisions.*

REFERENCES

(1) Wikipedia's "Radio-frequency identification" page, http://en.wikipedia.org/wiki/Radio-frequency_identification

(2) Wireless Telegraphy Act 2006, http://www.legislation.gov.uk/ukpga/2006/36/pdfs/ukpga_20060036_en.pdf

(3) Office of Communications ("OFCOM"), http://www.ofcom.org.uk/

(4) Wireless Telegraphy (Radio Frequency Identification Equipment) (Exemption) Regulations 2005 (SI 2005/3471) (2005 Regulations), http://www.legislation.gov.uk/uksi/2005/3471/pdfs/uksi_20053471_en.pdf

(5) Decision 2006/804/EC, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:329:0064:0066:FR:PDF

(6) Wireless Telegraphy (Radio Frequency Identification Equipment (Exemption) (Amendment) Regulations 2007 (SI 2007/1282) http://www.legislation.gov.uk/uksi/2007/1282/pdfs/uksi_20071282_en.pdf

(7) Data Protection Act 1998 http://www.legislation.gov.uk/ukpga/1998/29/data.pdf

(8) Information Commissioner's Office (ICO), www.ico.org.uk

(9) ICO's Data Protection Technical Guidance - Radio Frequency Identification, 09.08.06.

DANNY PREISKEL

Les réseaux d'objets intelligents

▪ Les réseaux d'objets intelligents (*smart medical devices*, *smart home devices*,…) n'ont pas cessé de se développer ces dernières années et de trouver de plus en plus d'applications concrètes et utiles dans la vie courante, loin des gadgets des débuts, réservés aux technophiles argentés.

▪ En mars 2010 déjà, nous avions rédigé un article faisant le point et tentant d'anticiper l'influence de l'Internet des Objets sur les législations en matière de vie privée **(1)**. Depuis lors, force est de constater que le cadre législatif belge – et même européen – entourant la protection de la vie privée n'a pas évolué du tout pour tenir compte de cette nouvelle réalité qui voit advenir un ensemble d'objets interconnectés récoltant, communiquant, croisant et traitant toujours plus de données personnelles, y compris les données les plus intimes, comme les données médicales.

▪ Pour l'heure, toute personne souhaitant développer un objet intelligent devra donc s'assurer que les traitements de données opérées par son produit respectent le prescrit de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel **(2)**.

▪ A l'échelon européen, la lecture de la recommandation de la Commission du 12 mai 2009 sur la mise en œuvre des principes de respect de la vie privée et de protection des données dans les applications reposant sur l'identification par radiofréquence **(3)** (soit la RFID, une des technologies utilisées dans le cadre de l'internet des objets) et de l'avis du Groupe 29 sur la proposition révisée des entreprises relative au cadre d'évaluation de l'impact sur la protection des données et de la vie privée des applications reposant sur l'identification par radiofréquence (RFID) **(4)** nous apprennent que les entreprises devraient prendre garde à l'ensemble des données traitées par ces technologies et non uniquement aux données à caractère personnel. En effet, bon nombre de données collectées n'ont pas nécessairement pour finalité d'être associée à une personne identifiée ou identifiable mais impliquent quand même un impact sur la vie privée des personnes et, singulièrement, des consommateurs.

▪ A l'échelon belge, seules les données à caractère personnel sont envisagées, notamment dans l'avis d'initiative du 28 octobre 2009 de la Commission de la protection de la vie privée relatif à la RFID **(5)**.

▪ Bien que bon nombre d'intervenants le perdent de vue, envisager les réseaux d'objets intelligents nécessitent d'aborder d'autres domaines juridiques que le droit de la vie privée, singulièrement depuis que les décisions autonomes prises par ces objets dits « intelligents » - et les dysfonctionnements qui y sont associés – peuvent sérieusement impacter leur environnement.

▪ L'on imagine ainsi aisément les conséquences potentiellement lourdes d'une décision prise par un défibrillateur personnel automatique, par un drone de livraison autonome ou encore par une voiture sans conducteur.

▪ Ces situations – et singulièrement les hypothèses d'accident en période intermédiaire avant l'automatisation totale, entre un engin manœuvré par un humain et une machine automatique – seront probablement génératrices de chaines complexes de responsabilité, mêlant responsabilité extracontractuelle (art. 1382-1383 du Code civil), responsabilité contractuelle (art. 1147 du Code civil), garantie des vices cachés (art. 1641 et s. du Code civil), responsabilité du fait des produits défectueux (loi du 25 février 1991),…

▪ A n'en pas douter, les questions de responsabilité – et d'assurance- liées à la mise sur le marché d'appareils toujours plus autonomes seront examinées par l'industrie avec encore plus d'acuité que les problématiques de vie privée.

REFERENCES

(1) Jean-François Henrotte, "Influence of the "Internet of Things" on Legislation regarding the Protection of individual Privacy", Palo Alto, CA, USA, Stanford LawSchool, Association for the Advancement of Artificial Intelligence, 23th March 2010

(2) Loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel

(3) 2009/387/CE, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:122:0047:0051:FR:PDF

(4) Avis 9/2011, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp180_fr.pdf

(5) Avis d'initiative relatif à la RFID (A/2009/003), http://www.privacycommission.be/sites/privacycommission/files/documents/avis_27_2009_0.pdf

JEAN-FRANÇOIS HENROTTE

The Networks of Smart Objects

▪ *Smart objects (smart medical devices, smart home devices,…) are increasingly interconnected with more and more concrete and useful applications in day-to-day life, no longer just for a happy few who are sufficiently tech-savvy and well-off, but for the average citizens.*

▪ *In March 2010, we already wrote an article taking stock of and trying to anticipate the impact of the Internet of Things on privacy laws* ***(1)****. Since then, it is clear that the Belgian - and even the European - legal framework regulating the protection of privacy has not changed at all to reflect this new reality that sees the birth of a variety of interconnected objects that collect, communicate, combine and process more and more personal data, including the most secret data such as medical data.*

▪ *For now, anyone wishing to develop an intelligent object therefore needs to ensure that the data processing carried out by the product complies with the requirements of the Belgian Act of 8 December 1992 on the protection of privacy with regard to the processing of personal data* ***(2)****.*

▪ *At the European level, it is apparent from the combined reading of the Commission Recommendation of 12 May 2009 on the implementation of privacy and data protection principles in applications supported by radio-frequency identification* ***(3)*** *(RFID is a technology used in the internet of Things) and the opinion of the Article 29 Working Party on the revised Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications* ***(4)*** *that companies should keep a watchful eye on all kinds of data processed by these technologies — and not only of personal data. Indeed, while many of the data collected are not necessarily intended to be associated with an identified or identifiable person, they can still have an impact on the privacy of individuals in general and consumers in particular.*

▪ *At the Belgian level, though, only personal data are have been taken into account for the moment, in particular by the Belgian Commission for the protection in its privacy's own-initiative opinion of 28 October 2009 on RFID* ***(5)****.*

▪ *We must not lose sight that networks of smart objects should be considered not exclusively through the lens of privacy, as the autonomous decisions taken by the so-called "smart" objects - and all related misuse and/or errors - can seriously impact their environment.*

▪ *It is easy to imagine the potentially serious consequences of a decision taken by an automatic home defibrillator, by an autonomous delivery drone or by a driverless car.*

▪ *These situations - and especially the interim period, i.e. the one taking place before the achievement of full automation, sandwiched between a human-operated machine and an automatic machine - will probably generate complex chains of liability, combining tort (Art. 1382 to 1383 of Belgian Civil Code), contractual liability (Art. 1147, Civil Code) warranty against hidden defects (Article 1641 et seq., Civil Code), liability for defective products (Belgian Law of 25 February 1991), just to name a few.*

▪ *The time will definitely come when the issues of liability and — insurance — raised by the marketing of increasingly autonomous devices will be considered by undertakings and other stakeholders with even more acuteness than the issue of privacy.*

(1) Jean-François Henrotte , "Influence of the "Internet of Things" on Legislation regarding the Protection of individual Privacy", Palo Alto, CA, USA, Stanford LawSchool, Association for the Advancement of Artificial Intelligence, 23th March 2010

(2) Loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel

(3) 2009/387/EC, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:122:0047:0051:EN:PDF

(4) Opinion 9/2011, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp180_en.pdf

(5) Avis d'initiative relatif à la RFID (A/2009/003), http://www.privacycommission.be/sites/privacycommission/files/documents/avis_27_2009_0.pdf

JEAN-FRANÇOIS HENROTTE

- L'Internet des objets, désigné comme la 4e révolution de l'Internet après la connectivité, le e-commerce et les réseaux sociaux, sera sans aucun doute, la technologie de notre quotidien dans le futur. Un monde où tout est connecté, avec des transmissions de données à chaque instant, présente beaucoup d'avantages pour les consommateurs, mais comme toute technologie, également de nombreux inconvénients.
- Cette nouvelle technologie, qui implique de nouveaux fournisseurs de services, des nouveaux systèmes de sécurité, une interaction inédite entre les dispositifs et les infrastructures, tous caractérisés par l'intelligence artificielle, changera assurément les relations des humains avec les objets qui les entourent, créant une nouvelle société. Cette nouvelle société, grande consommatrice des réseaux de télécommunications et des radiofréquences (y compris du spectre libre et non réglementé) permettra aux entreprises d'avoir accès à un nombre incalculable de données personnelles concernant les utilisateurs d'objets intelligents.
- Dans ce contexte : Comment protéger la vie privée ? Comment contrôler l'utilisation des données personnelles par les entreprises ? Et plus généralement, comment garantir la sécurité de tous dans le monde du futur ?
- Les enjeux juridiques de l'IdO sont énormes. Sur le plan de la responsabilité, tout d'abord, la multiplication des technologies (RFID, entre autres) et des dispositifs interconnectés rend plus ardue l'identification des rôles et des responsabilités de chacun, et notamment des fournisseurs de services de l'IdO, et donc complexifie l'imposition de limites à tous les acteurs concernés. Les conséquences : une vulnérabilité accrue des consommateurs, des contentieux avec une facturée de plus en plus salée, et des procédures d'audit incroyablement complexes. Lorsque les objets prendront des décisions pour l'homme, il conviendra d'appréhender et de concilier les droits créés et les obligations générées par une action ou une décision prise par une machine. Quid du cas où une voiture intelligente, percutant une autre voiture ou une personne, causera un accident susceptible de causer la mort d'un conducteur, d'un passager ou d'un piéton ? Sur le plan de la sécurité, la protection des données personnelles et de la vie privée des utilisateurs est bien évidemment en jeu : des cybercriminels peuvent accéder à un appareil, le contrôler à distance, accéder aux données personnelles qu'il contient et les divulguer sur Internet, le tout à l'insu de l'utilisateur, du fournisseur de services et même du contrôleur de radiofréquence. Plus généralement, il en va également de la sécurité publique des personnes : imaginez si des criminels pouvaient accéder aux systèmes de votre voiture et ainsi savoir où vous vivez, à quelle heure vous arrivez chez vous, où vous travaillez, où vos enfants vont à l'école…
- Au Brésil, l'internet des objets n'en n'est qu'à ses débuts. Son utilisation est encore limitée, même dans le secteur de la logistique, et ce n'est qu'en 2013 que sont apparus quelques rares objets intelligents, pour la plupart des appareils ménagers : réfrigirateurs, cuisinières, systèmes d'éclairage, moniteurs pour bébé... contrôlables à distance, le plus souvent via des appareils mobiles grâce à un système qui permet à l'utilisateur de les programmer à partir de leurs smartphones. L'internet des objets a beau être considéré comme l'avenir du quotidien, il n'en reste pas moins qu'au Brésil, aujourd'hui, cette technologie n'est pas encore très répandue. Outre le manque d'infrastructures, la raison en est que les dispositifs intelligents n'offrent pour l'instant que des fonctions simples, mais néanmoins très coûteuses, accessibles seulement à une petite partie de la population. Selon une étude de l'Union internationale des télécommunications (UIT) menée en 2013 **(1)**, le Brésil figure à la 62ème position dans la liste des 157 pays les plus connectés. Cette étude se fonde sur le niveau des infrastructures et sur l'accès et l'utilisation des réseaux Internet et mobile. Même si ce résultat n'est pas mauvais, le Brésil a encore beaucoup de progrès à faire afin d'entrer de plain-pied dans l'Internet des objets.
- Sur le plan législatif, le Brésil n'a toujours pas adopté un cadre spécifique pour protéger les données à caractère personnel **(2)** ni même un texte encadrant l'Internet, et a fortiori l'Internet des objets. Un projet de loi Internet est toutefois en cours de discussion par le Parlement brésilien **(3)**. En attendant, il est possible de régler les problématiques qui se présentent au moyen des lois existantes, car si la plupart des services ou situations liés à l'internet des objets ne sont pas réglementés par une loi spécifique, la majeure partie des activités concernées bénéficient toutefois d'une protection juridique directement ou indirectement par le biais des droits personnels, du droit de la consommation et du droit de la responsabilité (civile et commerciale).
- L'internet des objets n'est donc pas encore une réalité au Brésil. Pour autant il serait pertinent de d'ores et déjà anticiper son développement. Il est important que le pouvoir législatif et le pouvoir exécutif soient pleinement mobilisés et engagent un travail en commun en vue de créer des politiques publiques aptes à faire progresser le Brésil sur les plans législatif et technique (systèmes de sécurité, infrastructures réseau) afin de relever les défis de l'IdO.

REFERENCES

(1) International Telecommunication Union "Measuring the Information Society" (MIS Report), édition 2013, rapport complet (anglais) et résumé analytique (français).

(2) Marco Civil da Internet (portugais, et traduction anglaise non officielle)

(3) Anteprojeto de Lei de Proteção de Dados Pessoais (portugais)

SILVIA REGINA BARBUY MELCHIOR

- *The Internet of Things, also known as the 4º revolution of internet – preceded by the first steps of connectivity, the e-commerce and the social networks -, is certainly the future of our day-to-day technology. In the perspective of a world where everything is connected and our whole routine is based on data transmission, we can point out lots of benefits and amenities for the consumer, but, as any other technology, we can also forecast lots of implications and misapplication too.*
- *This new technology also involves new service providers, security systems, interaction of devices and infrastructure, all of them characterized by artificial intelligence which at least will change the interaction between humans and machines creating a new society. In one hand this new society demands lots of resources in terms of telecommunication networks and radiofrequency, including free and non-regulated spectrum - and on the other hand enables companies to have access to lots of personal data of the users.*
- *But there are still lots of questions to be answered: how privacy and personal data will be protected? How control companies in the usage of personal information? How achieve a security society?*
- *Actually considering that several devices and tags (with technologies such as RFID) connected supporting different services will be connected it will be more and more difficult to identify responsibilities and limits for each service provider. The vulnerability of consumer will be even higher than is today. Litigation will be even more expensive and based on complexes auditing process. Devices will take decisions in the name of humans (as in the case of a smart car which is in a situation involving more than two risks events - hit another car or a person – causing the death of a person in both situations). How evaluate and balance different rights and the effects caused by a particular action or decision made by a machine and which right we will accept to be affected. Furthermore in the field of cybercrime it is possible to imagine hackers that can access the device and control it remotely without the permission of the user, the service provider or even the radiofrequency controller (infrastructure) or accessing personal data an sharing it on the internet. The worries are not only with the personal data and privacy of the users, but we can also forecast public security problems too with the development of the technology. Imagine if organized crime can access car systems and know where people live, what time they get home, where they work, where their children study.*
- *In Brazil, the Internet of Things is on its first steps. It is not widely used in logistic and only in 2013 it began to be launched some few intelligent devices, most of them related with house appliances - refrigerators, stoves, light systems and baby monitors that can be remotely controlled -, mainly connected with mobile devices through a system that allows the user to program them from smartphones. Although the Internet of Things is seen as the future of people's day-to-day living, here in Brazil, the technology is not yet widespread; the lack of infrastructure is a challenge to be overcome; the intelligent devices have only simple functions and are very expensive, only accessible to a small portion of the population. Accordingly to the International Telecommunication Union (ITU) research (2013) **(1)**, Brazil is in the 62th position of the 157 countries more connected. It shows the level of infrastructure, access and use of internet and mobile. Even though it is not bad, Brazil has a lot of work to do enable Internet of Things.*
- *In terms of legislation, Brazil still does not have a specific framework to protect personal data **(2)** or even a regulation on Internet or Internet of Things. Brazilian congress is discussing the approval of the Internet Bill **(3)** while raising problems are being solved by existing laws. Despite of most part of the set of service/implications related to Internet of Things is not subject to specific law the major part of activities involved is under legal protection as personal rights, consumer protection, civil or commercial responsibilities or maintains connection with areas of law indirectly applied.*
- *Although the Internet of Things is not yet a reality in Brazil, we recognize that is relevant to consider the appropriate approach. It is important that the legislative and the executive powers work together to create public policies to improve, not only our legislation, but also our security systems and infrastructure of network to support the new demands that might overload our system.*

REFERENCES

(1) International Telecommunication Union "Measuring the Information Society", (MIS Report), Edition 2013

(2) Marco Civil da Internet (portuguese, and unofficial English translation)

(3) Anteprojeto de Lei de Proteção de Dados Pessoais (portuguese)

SILVIA REGINA BARBUY MELCHIOR

LANGLOIS, KRONSTRÖM, DESJARDINS

Enjeux juridiques de l'Internet des objets au Canada

▪ Le phénomène de l'explosion des données, l'arrivée de l'ère du Big Data et du développement des procédés d'analyse (data mining) étaient surtout attribuables à la hausse de l'utilisation des technologies de l'information par des personnes, ainsi qu'à l'amélioration de la connectivité et à l'augmentation de la capacité de stockage et de traitement des données.

▪ Le déploiement de ce que l'on appelle l'Internet des objets, soit la détection, la collecte, la communication machine-à-machine et le traitement automatisé de données par toute une panoplie d'objets que nous utilisons directement ou accessoirement, que ce soit des véhicules, la mécanique des bâtiments, des infrastructures, des électroménagers, des instruments de paiements, système de gestion d'inventaire, ou des systèmes de sécurité, constitue la source de son inévitable expansion.

▪ L'Internet des objets présente un potentiel d'optimisation dans de nombreuses sphères d'activités, dont la consommation d'énergie, le transport, les soins de santé, et le partage des ressources, mais soulève par ailleurs de nombreux enjeux techniques, sociaux, et juridiques.

▪ Parmi les enjeux juridiques soulevés par les différentes applications des communications machine-à-machine, on peut penser à l'encadrement de la publicité ciblée en ligne, à l'encadrement de la gestion des risques par les assureurs, à la détermination de la responsabilité en cas de sinistres attribuables aux fonctions de contrôle attribuées aux objets, ainsi qu'aux risques liées à la sécurité des personnes et à la protection de la vie privée, dont les paramètres d'obtention d'un consentement éclairé, la responsabilité pour les brèches de sécurité, et la reconnaissance d'un droit à la non connectivité.

▪ À ce jour, le gouvernement canadien s'est principalement intéressé au phénomène sous l'angle du développement économique et des opportunités pour l'industrie canadienne du numérique **(1)**. Au cours de l'année 2010, le gouvernement du Canada a publié un document de consultation sur sa Stratégie sur l'économie numérique **(2)**, et obtenu de nombreuses interventions. Certaines interventions ont notamment insisté sur l'importance de favoriser des standards ouverts et d'éliminer les barrières aux transferts transfrontaliers de données **(3)**, afin de maximiser les opportunités liées à l'internet des objets Le Bureau de la consommation a par ailleurs publié un document d'information sur le développement et le déploiement des technologies RFID au Canada et sur les préoccupations des consommateurs **(4)**.

▪ L'étude des enjeux liés à la protection de la vie privée est à ce jour principalement attribuable aux autorités canadiennes chargées de la protection de la vie privée. Le Commissariat à la protection de la vie privée a ainsi élaboré des recommandations sur l'utilisation de la technologie RFID en milieu de travail **(5)**, notamment en regard des méthodes d'obtention du consentement en insistant sur le fait : « qu'il incombe aux organismes d'informer les personnes des buts principaux et secondaires qui motivent la collecte, l'utilisation et la communication de tout renseignement personnel, ainsi que des options qui s'offrent à ces personnes dans des cas particuliers, y compris la possibilité de se retirer d'un projet précis de collecte, d'utilisation ou de communication de renseignements personnels. »

▪ La commission d'accès à l'information du Québec (la « CAI ») a publié dès 2006, un document d'analyse sur les technologies d'identification par radiofréquence **(6)**. Dans son rapport quinquennal publié en 2011 la CAI recommandait au législateur de modifier les lois applicables aux secteurs public et privé de façon à imposer expressément l'obligation de signaler « la présence de mécanismes susceptibles d'identifier ou de localiser une personne physique » en regard de produits présentant de telles fonctionnalités **(7)**.

▪ La Commissaire à la vie privée de l'Ontario a également publié des Lignes directrices régissant la protection de la vie privée pour les systèmes d'identification par radiofréquence ainsi que des Lignes directrices pour les prestataires des soins de santé **(8)**.

▪ La Commissaire ontarienne s'est plus récemment engagée dans les consultations publiques sur les enjeux de l'internet des objets lancées par le Département du Commerce Américain **(9)** et la Federal Trade Commission **(10)** en insistant sur la nécessité d'adopter une approche fondée sur la protection intégrée de la vie privée (Privacy by design) dans l'élaboration de normes destinées à encadrer l'Internet des objets.

▪ Ainsi, bien que les principes généraux énoncés dans les lois canadiennes vouées à la protection des renseignements personnels puissent permettre d'encadrer certains aspects des enjeux juridiques soulevés par l'internet des objets, le cadre juridique canadien reste à définir.

REFERENCES

(1), Horizons de politiques Canada, Qu'est ce qui stimule le système économique international en évolution ?, Gouvernement du Canada, avril 2013.

(2) Gouvernement du Canada, Accroître l'avantage numérique du Canada, 2010

(3) Instrumented, Interconnected and Intelligent — IBM Canada's Perspective on a Digital Economy Strategy, 2010; GS1 Canada, Advancing the "Internet of Things" - Digital Economy Strategy Submission to Industry Canada, 2010.

(4) Bureau de la consommation, Les technologies RFID et les consommateurs sur le marché de la vente au détail, Industrie Canada, 2007

(5) Commissariat à la protection de la vie privée au Canada, L'identification par radiofréquence (IRF) en milieu de travail : Document de consultation sur les recommandations de règles de pratique et Résultats de la consultation, CPVPC; 2008–2010

(6) Commission d'accès à l'information du Québec, La technologie d'identification par radiofréquence (RFID) doit-on s'en méfier ?, Mai 2006

(7) Commission d'accès à l'information du Québec, Rapport quinquennal 2011 – Technologies et vie privée : à l'heure des choix de société, p. 28

(8) Ann Cavoukian, Lignes directrices régissant la protection de la vie privée pour les systèmes d'identification par radiofréquence, IPCO, Juin 2006. IPCO, RFID and Privacy: RFID and Privacy: Guidance for Health-Care Providers, Janvier 2008.

(9) Ann Cavoukian, Submission of the Information and Privacy Commissioner of Ontario - Response to the Department of Commerce Internet Policy Task Force's proposed framework for Commercial Data Privacy and Innovation in the Internet Economy. IPCO, Janvier 2011

(10) Ann Cavoukian, Submission of the Information and Privacy Commissioner of Ontario - Response to the FTC call for input on the privacy and security implications of the Internet of Things, IPCO, Avril 2013

JEAN-FRANÇOIS DE RICO

Legal stakes of Internet of Things in Canada

▪ *The phenomenon of the explosion of data, the arrival of the era of Big Data and the development of analysis processes (data mining) were mainly attributable to the increased use of information technologies by individuals, as well as to the improvement of connectivity and the increase of the storage and data processing capacity.*

▪ *The deployment of what is called the "Internet of things", in other words the detection, collection, machine-to-machine communication and automatic processing of data by a variety of things we use directly or indirectly, such as vehicles, building mechanics, infrastructures, appliances, payment instruments, inventory management systems, or security systems, is the source of its inevitable expansion.*

▪ *The Internet of Things has the potential to optimize many spheres of activities, including energy, transportation, health care, and the sharing of resources, but it also raises many technical, social and legal challenges.*

▪ *Among the legal issues raised by the various applications of Machine-to-Machine communications, one can think of the regulation of targeted online advertising, the supervision of risk management by insurers, the identification of responsibility in case of loss due to the defective control functions of things, as well as risks related to the safety of persons and the protection of privacy (informed consent, liability for security breach, recognition of a right to non connectivity).*

▪ *To date, the Canadian government has mainly focused on the phenomenon in terms of economic development and opportunities for Canada's digital industry* ***(1)****. During 2010, the Government of Canada released a consultation paper on its Digital Economy Strategy* ***(2)****, and received numerous contributions. Some contributors stressed the particular importance of promoting open standards and eliminate barriers to cross-border data transfers* ***(3)*** *to maximize the opportunities associated with the Internet of Things. The Office of Consumer Affairs (OCA) also published a document about the development and deployment of RFID technologies in Canada and consumer concerns* ***(4)****.*

▪ *So far, the privacy-related issues of IoT have mainly been studied by the Canadian authorities in charge of the protection of privacy. The Office of the Privacy Commissioner of Canada has developed recommendations on the use of RFID technology in the workplace* ***(5)****, particularly in relation to methods for obtaining consent insisting on the fact "that organizations have primary responsibility to inform individuals about the primary and any secondary purposes motivating a collection, use or disclosure of any personal information, as well as their options in a particular information bargain, including any ability to opt out of a particular collection, use or disclosure of personal information".*

▪ *In 2006, Quebec's Access to Information Committee ("CAI") issued an analysis on RFID technology* ***(6)****. In its five-year report released in 2011, the CAI recommended that the legislator oblige bodies from the public and private sectors to report "the presence of mechanisms likely to identify or locate a natural person" during use of products with such features* ***(7)****.*

▪ *The Office of the Information and Privacy Commissioner of Ontario has also published Guidelines on the protection of privacy in the RFID systems as well as Guidelines for health care providers* ***(8)****.*

▪ *The Ontario Commissioner has recently engaged in public consultations on the issues of the Internet of Things launched by the U.S. Department of Commerce* ***(9)*** *and the Federal Trade Commission* ***(10)*** *emphasizing the need for an approach based on integrated privacy protection (privacy by design) in the development of standards to regulate the Internet of Things.*

▪ *Thus, although the general Canadian principles enshrined in the protection of personal information legislation can help to regulate certain aspects of the legal issues raised by the Internet of Things, the Canadian legal framework still remains to be created.*

REFERENCES

(1), Policy Horizons Canada, What's Driving the Evolving International Economic System?, Government of Canada, April 2013.

(2) Government of Canada, Improving Canada's Digital Advantage, 2010

(3) Instrumented, Interconnected and Intelligent — IBM Canada's Perspective on a Digital Economy Strategy, 2010; GS1 Canada, Advancing the "Internet of Things" - Digital Economy Strategy Submission to Industry Canada, 2010.

(4) Office of Consumer Affairs, RFID Technologies and Consumers in The Retail Marketplace, Industry Canada, 2007

(5) Office of the Privacy Commissioner of Canada, Radio Frequency Identification (RFID) in the Workplace: A Consultation Paper on Recommendations for Good Practices et Consultation Results, OPC; 2008–2010

(6) Commission d'accès à l'information du Québec, La technologie d'identification par radiofréquence (RFID) doit-on s'en méfier ?, Mai 2006

(7) Commission d'accès à l'information du Québec, Rapport quinquennal 2011 – Technologies et vie privée : à l'heure des choix de société, p. 28; (in French)- (Summary in English)

(8) Ann Cavoukian, Privacy Guidelines for RFID Information Systems (RFID Privacy Guidelines), IPC, June 2006. IPC, RFID and Privacy: Guidance for Health-Care Providers, January 2008.

(9) Ann Cavoukian, Submission of the Information and Privacy Commissioner of Ontario - Response to the Department of Commerce Internet Policy Task Force's proposed framework for Commercial Data Privacy and Innovation in the Internet Economy. IPC, January 2011

(10) Ann Cavoukian, Submission of the Information and Privacy Commissioner of Ontario - Response to the FTC call for input on the privacy and security implications of the Internet of Things, IPCO, Avril 2013

JEAN-FRANÇOIS DE RICO

▪ L'Internet des objets investit peu à peu tous les domaines, dans le monde entier, et il faut s'attendre à ce qu'il révolutionne les relations homme-à-objet et objet-à-objet dans les 10 prochaines années. C'est d'ailleurs dans ce dernier domaine que l'innovation sera la plus forte, grâce à l'utilisation croissante de la technologie RFID (Radio Frequency Identification). Au cœur de la technologie RFID se trouve le transpondeur (étiquette ou, plus fréquemment, « tag »), un composant électronique constitué d'une puce et d'une antenne. La puce permet notamment de stocker, recevoir et transmettre sans fil des informations sur la nature et la composition de l'objet sur lequel elle a été apposée. La combinaison des technologies RFID avec l'utilisation d'une adresse IP (Internet Protocol) ouvre la voie à une vaste gamme d'usages et d'applications. L'exemple le plus souvent cité est celui du réfrigérateur qui sera en mesure de communiquer à son propriétaire des informations sur les produits qu'il contient, et notamment sur leurs dates limites de consommation. Ces technologies, et leurs nouvelles applications, sont susceptibles de générer d'innombrables avantages économiques et sociaux, tout en constituant des enjeux importants en matière de sécurité et de confidentialité.

Guide de l'autorité espagnole de protection des données sur la RFID

▪ C'est dans ce contexte qu'en 2010, l'autorité espagnole de protection des données **(1)** a publié un guide sur la sécurité des données et la vie privée dans le cadre des technologies RFID **(2)**.

▪ Ce guide identifie plusieurs zones de risque liées à l'utilisation des technologies RFID et formule des recommandations pratiques à destination des utilisateurs et fournisseurs de ces technologies.

▪ Ont été ainsi désignées comme menaces potentielles : l'isolation des tags, afin d'empêcher une bonne communication entre le lecteur et le tag ; l'usurpation d'identité, par l'envoi de fausses informations ; les dénis de service (DoS), qui saturent le système par l'envoi de demandes de communication externe ; la destruction des tags en les exposant à un fort champ magnétique ; et les logiciels malveillants, par la transmission de codes malveillants dans le tag RFID.

▪ S'agissant plus particulièrement des données personnelles, l'autorité espagnole attire l'attention sur les risques pesant sur leur confidentialité et leur protection, et notamment l'accès et le traitement non autorisés de données contenues dans ces tags.

▪ L'autorité de protection espagnole a confirmé que la loi organique 15/1999 sur la protection des données à caractère personnel du 13 décembre 1999 **(3)** était pleinement applicable aux technologies RFID, dès lors qu'elles impliquent le traitement de données personnelles.

▪ En conséquence, les entreprises doivent se préparer à faire face aux différentes questions soulevées par les technologies RFID. Quelques pistes de réflexion à envisager : évaluer la nécessité de collecter ou stocker des données personnelles par le biais de ces technologies ; informer les personnes concernées des finalités et de l'utilisation des données traitées ; obtenir leur consentement dans le respect de la loi applicable ; prendre des mesures de sécurité appropriées. Sur ce dernier point, les actions envisagées vont du renommage des tags (pour éviter l'usurpation de l'identité d'une étiquette ou d'autres attaques similaires), au cryptage des données, en passant par l'authentification et la minimisation des données, l'intégration de mentions d'informations pertinentes et la possibilité de désactiver ou de retirer le tag. Les entreprises qui utilisent les technologies RFID sont invitées à intégrer ces mesures dans leur gestion globale des risques.

▪ Quant aux utilisateurs de produits intégrant la RFID, ils doivent être sensibilisés à ces technologies et bien connaître leurs droits à la protection de leur vie privée et de leurs données personnelles. Afin de garantir leur sécurité, ils devraient adopter des mesures spécifiques lorsqu'ils utilisent des technologies RFID, parmi lesquelles la mise en place de tags de surveillance (qui les informent sur les tentatives non autorisées de lecture et d'écriture des tags), la mise en œuvre de mesures d'isolement (pour empêcher des périphériques externes d'accéder aux informations contenues dans l'étiquette), ou l'utilisation de pare-feu RFID. Ces mesures ne sont pas exhaustives et les utilisateurs doivent rester vigilants afin de protéger leurs droits.

REFERENCES

(1) Agencia Española de Protección de Datos, www.agpd.es

(2) Guía sobre seguridad y privacidad (en espagnol et en anglais)

(3) Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal (version espagnole et traduction française)

MARC GALLARDO

▪ *The Internet of Things is becoming ever more popular worldwide and in the next 10 years is set to revolutionise person-to-thing and thing-to-thing interaction – where the innovation really lies thanks to the growing use of RFID (radio frequency identification) technologies. The key element in RFID technology is the transponder (or tag), which is an electronic component consisting of a chip and an antenna. The chip can store, receive and transmit wirelessly information on the nature and composition of the product to which it has been applied. If RFID technologies are combined with an IP (Internet protocol) address we can foresee a huge range of uses and future applications. The most cited practical example of this is that of fridges which, if suitable programmed, will be able to detect any product past its use-by date, or approaching this, and will inform the consumer. These technologies and its new applications will give innumerable opportunities to produce economic and societal benefits but it will also trigger security and privacy concerns.*

The Spanish DPA's Guide on RFID

▪ *In 2010, the Spanish DPA* ***(1)*** *published a Guide on Security and Privacy of RFID technologies* ***(2)****.*

▪ *The Guide identifies several risks related to the use of RFID technologies, especially in the field of security and privacy and provides guidance in the form of practical recommendations for both users and providers of such technologies.*

▪ *Security risks mentioned in the Guide are: tags isolation - to avoid proper communication between the reader and the tag, impersonation - sending false information that seems to be valid, Denial of Service attack (DoS) – by saturating the system with external communications requests, tags destruction by putting down RFID tags in a strong magnetic field and malware – transmitting malicious codes inside the RFID tag's.*

▪ *Privacy risks also described in the Guide focus on unauthorized access to personal data stored in the tags and the non-informed or non-authorized processing of personal data contained in such tags for individual tracking.*

▪ *The Spanish DPA confirms that Organic Law 15/1999, of 13 December on the Protection of Personal Data (****3****) is fully applicable to the use of RFID technologies that process personal data.*

▪ *Companies using RFID technologies should assess the need to collect or store personal data through such technologies; inform data subjects on the purposes and uses of the data that will be processed, obtain their consent according to the Law and take appropriate security measures such as tag rename - to avoid impersonation of a tag or similar attacks; data encryption; authentication and data minimization; notification of the use of RFID technologies and, if available, the option to deactivate or remove the tag. Companies using RFID technologies should have to include these requirements into their risk management concept governing the business activities in general.*

▪ *Users should be aware of these technologies and have a proper knowledge of their rights to privacy and data protection in the RFID environment. On the security side, they should also consider additional measures to protect their privacy when using RFID technologies, such as the use of watchdog tags – that inform about the attempts to read and write the tags; isolation – to avoid external devices to access the information contained in the tag, or the use of firewall RFID, among others.*

REFERENCES

(1) Agencia Española de Protección de Datos, www.aqpd.es

(2) Guía sobre seguridad y privacidad (in Spanish and in English)

(3) *Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal (in Spanish and English)*

MARC GALLARDO

Actualité de l'Internet des objets aux Etats-Unis

▪ L'Internet des objets a le potentiel de transformer de nombreux secteurs, aussi divers et variés que la domotique, la médecine, ou encore les transports. Il permet de relier plus de choses et plus de personnes à l'Internet, et en fin de compte, plus de personnes les unes aux autres. Nos appareils sauront, plus que jamais, qui nous sommes, ce que nous achetons, ce que nous signons, et avec qui. D'où l'une des questions majeures soulevées par l'Internet des objets : la protection de la vie privée et la sécurité des données.

▪ En effet, les appareils et les services interconnectés dans le cadre de l'Internet des objets recueillent et partagent constamment de vastes quantités de données personnelles. Le législateur, les entreprises, et la communauté scientifique en général doivent donc veiller à la mise en place de mesures appropriées permettant de garantir la vie privée et la sécurité des utilisateurs et éviter les dérives dont ils pourraient être victimes.

▪ L'action récente de la Federal Trade Commission (FTC) contre la société TRENDnet **(1)** fournit un exemple édifiant des dysfonctionnements pouvant se produire lorsque des mesures de confidentialité et de sécurité appropriées font défaut. En l'espèce, la société TRENDnet commercialise des caméras de surveillance connectées à Internet dénommées « SecurView », pouvant être utilisées aussi bien pour assurer la sécurité d'une habitation que pour la vidéosurveillance de bébés. Or, suite à une faille logicielle, toute personne en possession de l'adresse IP d'une de ces caméras pouvait visualiser, voire dans certains cas écouter, les informations qu'elle transmettait en ligne. Des pirates ont ainsi publié en ligne, et en direct, les signaux émis par près de 700 caméras de particuliers, dévoilant en temps réel les activités de leurs utilisateurs (bébés endormis dans leur berceau, adultes vaquant à leurs occupations quotidiennes). En outre, il s'est avéré que la société TRENDnet avait transmis les identifiants des utilisateurs en texte clair et lisible sur Internet. TRENDnet s'est ainsi fait épinglée par le gendarme américain de la concurrence et de la protection des consommateurs. Pour la FTC, les pratiques de sécurité laxistes de la société TRENDnet ont violé la vie privée des centaines de consommateurs, en rendant possible la consultation publique de leurs données sur l'Internet. Elle a par ailleurs constaté que les pratiques de TRENDnet étaient trompeuses et déloyales. L'accord **(2)** finalement conclu entre la FTC et TRENDnet impose à cette dernière d'établir un programme exhaustif de sécurité de l'information et de se soumettre à un audit tiers tous les deux ans, pendant les 20 prochaines années. TRENDnet est également tenue d'informer les clients sur les questions de sécurité soulevées par ses caméras ainsi que de la disponibilité de mises à jour logicielles destinées à les corriger, et de fournir une assistance technique gratuite pour les deux prochaines années afin d'aider ses clients à mettre à jour ou de désinstaller les cameras.

(1) Marketer of Internet-Connected Home Security Video Cameras Settles FTC Charges It Failed to Protect Consumers' Privacy, www.ftc.gov, 04-09-2013.

(2) http://www.ftc.gov/sites/default/files/documents/cases/2013/09/130911trendnetfrn.pdf

▪ Par ailleurs, les appareils mobiles et les appareils portables jouent un rôle important dans l'Internet des objets. En effet, ils recueillent, analysent et partagent des informations sur les utilisateurs et leur environnement (emplacement actuel, habitudes de déplacement, vitesse, niveaux sonore du bruit ambiant). Ils permettent aux utilisateurs de se connecter les uns avec les autres dans toutes sortes de situations, et de partager - sciemment ou non - une grande variété d'informations entre eux et avec le prestataire de services.

▪ C'est pourquoi les fournisseurs d'applications mobiles ont l'obligation d'informer leurs clients sur la collecte et l'utilisation des données les concernant. Cette obligation est notamment imposée par la Loi californienne sur la protection de confidentialité en ligne **(3)**. La FTC veille au respect de cette obligation.

(3) California Online Privacy Protection Act http://oag.ca.gov/privacy/COPPA

▪ A titre d'illustration, en février 2013, la FTC a enquêté sur les pratiques de Path, un réseau social qui permet aux utilisateurs de tenir un journal sur les moments forts de leur vie et de les partager avec leurs amis (jusqu'à 150). La FTC a reproché à l'application mobile de Path **(4)** de tromper les utilisateurs en collectant des informations personnelles, notamment celles contenues dans les carnets d'adresses de leur téléphone, sans les en informer et sans obtenir leur consentement. La FTC a estimé que la collecte de renseignements personnels à partir d'un téléphone mobile, sans information ou autorisation des personnes concernées, était susceptible de constituer une pratique trompeuse ou déloyale en vertu de la Loi sur la FTC. L'accord amiable **(5)** conclu entre Path et la FTC impose au réseau social d'établir un programme complet en matière de la vie privée et de se soumettre à un audit indépendant de ses pratiques en matière de confidentialité, et ce tous les deux ans pour les 20 prochaines années. Path devra également s'acquitter d'une amende de 800.000 $ pour mettre fins aux poursuites concernant les accusations de recueil illégal de données personnelles de mineurs sans le consentement de leurs parents.

(4) http://www.ftc.gov/sites/default/files/documents/cases/2013/02/130201pathinccmpt.pdf

(5) http://www.ftc.gov/sites/default/files/documents/cases/2013/02/130201pathincdo.pdf

▪ Cette affaire a des retombées évidentes pour les autres appareils connectés à Internet qui collectent des informations personnelles sur les utilisateurs, qui doivent ainsi informer les utilisateurs et obtenir leur autorisation. Il convient de s'interroger sur les modalités de transmission par les entreprises, sur le petit écran d'un téléphone, d'informations sur les données, parfois de nature très sensible, que ces dispositifs et applications recueillent, utilisent, et partagent.

▪ Dans le cas d'appareils ayant peu ou pas d'interface utilisateur, informer les consommateurs peut s'avérer compliqué. En effet, les outils de suivi d'activités ne sont dotés que d'interfaces utilisateurs très basiques, situées sur l'appareil lui-même. Par exemple, les ampoules intelligentes peuvent ne pas être équipées d'une interface utilisateur directement accessible au consommateur. Des questions similaires se posent pour d'autres appareils intelligents, tels que les montres, les bracelets ou les lunettes. La gestion des questions de confidentialité sur ces dispositifs nécessitera une innovation constante et constituera un défi pour les entreprises, les ingénieurs et le législateur.

▪ L'Internet est devenu l'un des moteurs de l'économie mondiale. En passe de transformer des industries entières et de changer nos relations avec les autres personnes, l'Internet des objets est autant porteur de promesses et que de difficultés, et soulève d'importantes questions au regard de la vie privée et de la sécurité des informations.

FRANÇOISE GILBERT

Internet of Things: Recent developments in the United States

▪ *The Internet of Things has the potential to transform many fields, including home automation, medicine, and transportation. It will connect more things and more people to the Internet, and ultimately, connect more people with each other. Our devices will know, more than ever, who we are, what we pay, what we sign up for, or with whom we interact. As a result, one of the significant issues raised by the Internet of Things is consumer privacy and data security.*

▪ *Because interconnected devices and services often collect and share large amounts of personal information, companies offering products as part of the Internet of Things must ensure that they safeguard the privacy and security of users. Policymakers and members of the technology community must also be sensitive to consumer privacy and data security issues.*

▪ *The recent Federal Trade Commission action against TRENDnet* ***(1)*** *provides a vivid example of the potential mishaps that can occur when proper privacy and security measures are missing. TRENDnet sold its Internet-connected SecurView cameras for purposes ranging from home security to baby monitoring. Defective software allowed unfettered online viewing and in some instances listening, by anyone with the camera's IP address. As a result, hackers posted live feeds of nearly 700 consumer cameras on the Internet, showing activities such as babies asleep in their cribs and adults going about their daily lives. In addition, TRENDnet transmitted user login credentials in clear, readable text over the Internet.*

(1) Marketer of Internet-Connected Home Security Video Cameras Settles FTC Charges It Failed to Protect Consumers' Privacy, www.ftc.gov, 04-09-2013.

▪ *The Federal Trade Commission charged that TRENDnet's lax security practices exposed the private lives of hundreds of consumers to public viewing on the Internet and found that TRENDnet's practices were deceptive and unfair. Among other things, the settlement* ***(2)*** *requires TRENDnet to establish a comprehensive information security program and to obtain third-party assessments of its security programs every two years for the next 20 years. TRENDnet must also notify customers about the security issues with the cameras and the availability of the software update to correct them, and provide free technical support for the next two years to assist customers in updating or uninstalling their cameras.*

(2) http://www.ftc.gov/sites/default/files/documents/cases/2013/09/130911trendnetfrn.pdf

▪ *Mobile devices and wearable devices play an important role in the Internet of Things, as well. They collect, analyze, and share information about users and their environment, such as their current location, travel pattern, speed, or the noise levels in their surroundings. They allow users to connect with each other in all sorts of settings, and share - knowingly, or not - a wide variety of information among themselves and with the service provider.*

▪ *Mobile app providers have an obligation to inform their customers about their collection and use. This is specifically required by the California Online Privacy Protection Act **(3)**. The Federal Trade Commission agrees, as well. In February 2013, the Federal Trade Commission investigated the practices of Path, a social network that allows users to keep journals about moments in their life and share them with up to 150 friends.*

▪ *In its complaint against Path **(4)**, the FTC identified circumstances where Path deceived users by collecting personal information, such as information from their address books, without the users' knowledge or consent. The FTC concluded that the collection of personal information from a mobile phone without disclosure or permission may be a deceptive or unfair practice under the FTC Act. The final consent decree **(5)** requires Path to establish a comprehensive privacy program and obtain independent privacy assessments every other year for the next 20 years. Path will also have to pay a fine of U.S. $800,000 to settle charges that it illegally collected personal information from children without their parents' consent.*

▪ *This case has obvious implications for other Internet-connected devices that collect personal information about users. Such technologies should include some way to notify users and obtain their permission. This raises questions of how businesses should convey, on the small phone screen, information about what data, sometimes of a highly sensitive nature, these devices and apps collect, use, and share.*

▪ *Providing notice to consumers may be complicated in the case of devices with a limited or no user interface. Activity trackers have only very basic user interfaces on the device itself. Smart light bulbs may not have any consumer-facing user interface. Similar issues arise with wearable devices, such as smart watches, wristbands or glasses. Addressing consumers' privacy concerns over such devices will present business, engineering, and policy challenges that will require constant innovation.*

▪ *The Internet has evolved to one of the most dynamic forces in the global economy. It is reshaping entire industries and changing the way we interact on a personal level. The Internet of Things promises even greater progress, but raises significant information privacy and security issues.*

(3) California Online Privacy Protection Act
http://oag.ca.gov/privacy/COPPA

(4)
http://www.ftc.gov/sites/default/files/documents/cases/2013/02/130201pathinccmpt.pdf

(5)
http://www.ftc.gov/sites/default/files/documents/cases/2013/02/130201pathincdo.pdf

FRANÇOISE GILBERT

Internet des objets, aspects juridiques

▪ Dans les années 90 personne ne croyait qu'internet serait une révolution sans précédent… dans les années 2000 la notion de web 2.0 était considérée comme un « coup marketing » **(1)**… malheureusement les années passent et les bons vieux réflexes critiques persistent… tel est le cas de l'Internet des objets relégué pour l'heure au rang de vrai faux futur gadget.

▪ L'internet des objets (« IdO ») est pourtant une réalité **(2)** mais les formes sous lesquelles il se présente aujourd'hui ne sont rien à côté de ce qu'il nous réserve et que l'on appelle : le véhicule, la maison ou même la ville intelligente **(3)**… bref le monde de l'objet intelligent ! **(4)**

▪ L'intérêt des objets est pris très au sérieux par les acteurs économiques… qui investissent par millions voire milliards dans le domaine sans que cela ne se sache vraiment **(5)**.

▪ Cette réalité a été prise en compte très tôt par l'Union européenne comme en témoigne la conférence ministérielle du conseil de l'Union européenne des 6 et 7 octobre 2008. Mais il y a mieux avec la publication, le 18 juin 2009, d'une communication de la Commission au parlement européen, au conseil, au comité économique et social européen et au comité des régions intitulée précisément : « Internet des objets – Un plan d'action pour l'Europe » **(6)**.

▪ Au sein de cette communication 14 lignes d'action ont été retenues parmi lesquelles figurent :

- la nécessaire mise en œuvre d'une gouvernance au moins au plan européen ;
- la sécurisation de l'IdO principalement confié à l'ENISA ;
- le couple IdO et infrastructure d'importance vitale ;
- la nécessaire normalisation des technologies de l'IdO ;
- l'importance de la R&D et le lancement de projets pilotes ;
- la coopération du public et du privé sous forme de partenariats ;
- la sensibilisation des institutions au sein de l'Union ;
- le dialogue international ;
- la gestion des déchets et le recyclage ;
- la mesure d'acceptation, notamment l'exposition aux ondes électromagnétiques ;
- le suivi de l'internet des objets dont nous ne sommes encore qu'aux prémisses et qui évoluera nécessairement.

▪ Sur le plan juridique la communication évoque deux problématiques juridiques :

- La ligne d'action 2 – Evoque la nécessité d'un « Suivi du contenu des questions relatives à la vie privée et à la protection des données personnelles. Il s'agit là assurément d'une ligne d'action purement juridique ».
- La ligne d'action 3 – Retient le besoin de reconnaître le droit à la déconnexion autrement appelé le droit au « silence des puces ».

REFERENCES

(1) Eric Barbry, "Web 2.0: nothing changes … but everything is different": Communications & Strategies n° 68, First quarter 2007, special issue "Web 2.0: the internet as a digital common", Disponible sur SSRN : http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1009136

(2) Aujourd'hui, un utilisateur moyen dispose d'au moins deux objets connectés à l'internet et ce chiffre devrait passer à sept d'ici à 2015, date à laquelle la planète comptera 25 milliards de dispositifs avec une connexion sans fil. D'ici à 2020, ce chiffre pourrait doubler pour atteindre 50 milliards (Communiqué de presse de la Commission européenne sur la consultation sur l'internet des objets, IP/12/360, 12-04-2012).

(3) Par exemple, la Google car, le service Smart home by Orange, les villes de New Songdo (Corée du Sud) et de Masdar (EAU).

(4) Il s'agit du Web 3.0. Le web 3.0 désigne les relations entre les hommes et les objets et vient fusionner avec les web 2.0 (relations des hommes entre eux) et 1.0 (relations des hommes à l'information). (Sénat, Rapport d'information n°443 du 20-03-2013. Audition d'Alain Bensoussan, p. 58).

(5) Les objets connectés devraient ajouter quelque 1.900 milliards de dollars de valeur à l'économie mondiale à l'horizon 2020, selon des estimations du cabinet Gartner, Communiqué de presse, 11-11-2013.

(6) Communication de la Commission au parlement européen, au conseil, au comité économique et social européen et au comité des régions : « Internet des objets – Un plan d'action pour l'Europe », COM(2009) 278 final, 18-06-2009.

▪ Mais aujourd'hui où en sommes-nous ? Nulle part, ou plus exactement encore et toujours à s'interroger sur le pourquoi du comment on pourrait éventuellement commencer à penser qu'il faudrait réguler la matière.

▪ Or sur le plan de la régulation il existe au moins deux facteurs possibles de blocage : la ressource technique disponible d'une part ; les données à caractère personnel d'autre part.

L'objet connecté

▪ L'internet des objets repose nécessairement sur la connexion des objets, ce qui pose un double problème technique : l'identification de l'objet connecté en premier lieu et la connexion de l'objet ainsi identifié.

▪ Le premier point nous ramène à la question des adresses IP et de l'ONS (object name system) ; la seconde de l'usage des radiofréquences RFID qui est pour l'heure la technologie dominante.

▪ Le contrôle de ces technologies est donc l'un des enjeux majeurs de l'internet des objets.

L'objet communiquant

▪ L'internet des objets c'est aussi de la donnée personnelle **(7)**. Ici les questions sont liées à la peur d'une certaine forme de « big brother » que pourrait induire l'IdO.

▪ A l'heure où tout le monde s'émeut du programme américain de surveillance « Risk » comment ne pas penser à l'immense pouvoir que détiendrait…. ou détiendra celui qui sera en mesure de contrôler l'internet des objets… **(8)**

▪ Sur cette question du droit des données personnelles la question se cristallise essentiellement autour de la question du droit au « silence des puces », concept proche des principes « opt in/opt out » revisité pour l'IdO **(9)**.

▪ Mais au-delà de la question du droit au silence ou de la parole des puces, la question est celle de la nécessité d'adopter une réglementation ad hoc sur l'internet des objets ou de laisser le marché s'organiser autour de pratiques … aussi « bonnes » que possible.

▪ Le risque serait alors, au motif légitime d'une préservation légitime du droit des personnes, de réguler trop fortement l'IdO à l'instar de ce qui se passe aujourd'hui pour la biométrie. Rappelons que la biométrie a le triste attribut d'être la seule technologie considérée comme suspecte **(10)** et qui relève par nature d'un régime d'autorisation préalable.

Conclusions… très provisoires

Si ces deux questions sont importantes, il faut s'attendre à ce que l'internet des objets bouleverse la donne juridique bien au-delà de ces seules questions **(11)**.

▪ D'autres questions devront également être traitées ou prises en compte comme celle de la responsabilité **(12)**, de la propriété intellectuelle ou encore de la sécurité **(13)**.

▪ Nous n'en sommes là qu'au début d'une nouvelle ère dans la grande Histoire du numérique…**(14)**

(7) Par exemple, le « quantified self ». Cf. « Quantified Self : comment mieux se connaître grâce à ses données » www.cnil.fr, 26-11-2013 et Céline Avigon, « Quantified self et internet des objets: nouveau paradigme du partage de données » 02-07-2013.

(8) « Internet des objets », Bernard Benhamou Défi technologiques, économiques et politiques, Revue Esprit, mars avril 2009.

(9) « Faut-il confier nos vies à des puces ? », Amaury Mestre de Laroque, marianne.net, 16-06-2013.

(10) « Les français plutôt réservés sur l'usage de la biométrie dans la vie quotidienne », étude du Crédoc présenté sur le site de la Cnil, 08-07-2013.

(11) Eric Barbry, « The Internet of Things, Legal Aspects »: Communications & Strategies, No. 87, 3rd Quarter 2012, pp. 83-100, Disponible sur SSRN : http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2304137 et Alain Bensoussan, vidéo « Le régime juridique de l'Internet des objets », Accenture MyDSI-Tv, 04-2012.

(12) Alain Bensoussan et Eric Barbry pour Centraliens, n°621 du 25-10-2012, « Le point de vue des hommes de loi : propriété et usage des données », numéro spécial « L'Internet des Objets "IdO? Idéaux?" »: http://www.alain-bensoussan.com/internet-des-objets-propriete-et-usage-des-donnees/2012/11/15/

(13) « Le réfrigérateur connecté, nouvelle cible des pirates informatiques » www.france24.com, Sébastien Seibt, 17-01-2014

(14) « L'Internet des objets es sans nul doute « LA » révolution du XXIe siècle ». (cf. Sénat, Rapport d'information n 784 du 26-09-2012. Intervention d'Eric Barbry, p. 31).

ERIC BARBRY

Internet of things, legal aspects

▪ *In the 1990s, nobody believed that the Internet was going to spark an unprecedented revolution… In the 2000s, the concept of Web 2.0 was seen as a marketing stunt* ***(1)****… Now, yet years later, here come the Internet of things; and not surprisingly it has been met by fierce criticism and dismissed as a future true/false gadget. There is nothing new under the sun.*

And yet, the Internet of Things ("IoT") is already a reality ***(2)*** *and its current forms are nothing compared to what future has in store for us: smart cars, smart homes or even smart cities* ***(3)*** *… In brief, smart things in a smart world!* ***(4)****.*

▪ *For economic operators, the Internet of things is a deadly serious thing… and they are putting millions — if not billions — in it, without people really knowing it.****(5)***

▪ *The European Union rapidly took an interest in IoT. For example, the European ministerial meeting held on 6 and 7 October 2008 was focused on the Internet of the Future with emphasis on the Internet of Things and the European Commission drafted on 18 June 2009 an important Communication on the Internet of Things.*

▪ *This Communication of 18 June 2009 from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, entitled to "Internet of Things: an action plan for Europe"* ***(6)****, lays down 14 lines of action, including:*

- *The implementation of a governance at least at the European level;*
- *The security of IoT, entrusted mainly to ENISA;*
- *The status of IoT as an infrastructure of vital importance;*
- *The necessary standardization of IoT technologies;*
- *The importance of R&D and the launch of pilot projects;*
- *The cooperation of public and private sectors in the form of partnerships;*
- *The institutional awareness within the EU;*
- *The international dialog;*
- *The management of waste and recycling.*
- *The acceptance level, including exposure to electromagnetic waves;*
- *The future developments of IoT, which is in constant evolution.*

▪ *Two lines of action are more particularly interesting from a legal perspective:*

- *Line of action 2 – It raises the necessity for a "continuous monitoring of the privacy and the protection of personal data questions"; and*
- *Line of action 3 – It underlines the need to be able to disconnect from the networked environment, i.e. achieve the "silence of the chips".*

▪ *Where are we today? Nowhere, or more exactly, we are still adopting a wait and see policy, debating again and again on the why and how to possibility starting regulating this area.*

▪ *Two pitfalls might stand in the way of a regulation: (i) the technical resources available and (ii) the issue of personal data.*

(1) *Eric Barbry, "Web 2.0: nothing changes … but everything is different": Communications & Strategies n° 68, First quarter 2007, special issue "Web 2.0: the internet as a digital common", Available at SSRN: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1009136*

(2) Today, an average person has at least 2 objects connected to the Internet and this is expected to grow to 7 by 2015 with 25 billion wirelessly connected devices globally. By 2020 that number could double to 50 billion. This means a possible future in which many everyday things are linked (Press release of the European Commission on the consultation on the Internet of things, IP/12/360, 12-04-2012).

(3) For example the Google car, the service Smart home by Orange, the cities of New Songdo (South Korea) and Masdar (UAE).

(4) This is Web 3.0. Web 3.0 refers to the relations between men and things and merged Web 2.0 (man-to-man) with 1.0 (man-to-information). (see French Senate, Information Report No. 443 dated 20-03-2013. Hearing of Alain Bensoussan, p. 58).

(5) Gartner predicts that by 2020, Internet of Things will create $1.9 trillion of economic value add, Press release, 11-11-2013.

(6) *Communication of 18 June 2009 from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: "Internet of Things: an action plan for Europe", COM(2009) 278 final, 18-06-2009.*

Connected things

▪ *The Internet of things requires that objects be connected and this raises a double technical question: (i) How to identify the connected object? and (ii) How to connect the object so identified?*

▪ *The first question involves concepts such as IP addresses and ONS (Object Name System); the second question refers to the use of RFID radiofrequencies, which is currently the dominant technology.*

▪ *Controlling this technology is one of the major stakes of the IoT.*

Communicating things

▪ *The Internet of things also implies the use of personal data* ***(7)****. The main fear here is the Big Brother scenario.*

▪ *There has been a general outcry against the U.S surveillance program "Risk" — but what kind of power could - or will - have the one who will control the Internet of things?* ***(8)***

▪ *Regarding personal data, the debate is mainly focused only the right to de-activate chips, also known as "the right to silence of the chips", a concept close to the "opt in/opt out" principles and revisited for the IoT.* ***(9)***

▪ *But beyond the right for the chips to speak or be silent, the question is the relevance of adopting an ad hoc regulation of the Internet of things or let the market organize itself with practices… as "good" as possible.*

▪ *The risk would then be to impose overly stringent rules on IoT, on the legitimate purpose of protecting the right of individuals, in the same manner as what is currently the case for biometrics, which is notoriously known as the only technology considered as suspect* ***(10)*** *and subject to a prior authorization.*

Tentative conclusion…

▪ *While the two above questions are essential, this is just a beginning and one should expect IoT to change the legal world* ***(11)****.*

▪ *Far more legal questions are raised, such as liability* ***(12)****, intellectual property and security* ***(13)****, to name but a few.*

▪ *We are just at the beginning of a new era in the Digital History…* ***(14)***

(7) For example, "quantified self". See "Quantified Self : comment mieux se connaître grâce à ses données", www.cnil.fr, 26-11-2013 and "Quantified self et internet des objets: nouveau paradigme du partage de données" Céline Avigon, 02-07-2013.

(8) « Internet des objets », Bernard Benhamou Défi technologiques, économiques et politiques, Revue Esprit, mars avril 2009.

(9) « Faut-il confier nos vies à des puces ? », Amaury Mestre de Laroque, marianne.net, 16-06-2013.

(10) « Les français plutôt réservés sur l'usage de la biométrie dans la vie quotidienne », Crédoc study presented on the Cnil website, 08-07-2013.

(11) Eric Barbry, « The Internet of Things, Legal Aspects »: Communications & Strategies, No. 87, 3rd Quarter 2012, pp. 83-100, Available at SSRN: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2304137; Alain Bensoussan, video "Le régime juridique de l'Internet des objets", Accenture MyDSI-Tv, 04-2012.

(12) *Alain Bensoussan and Eric Barbry in* Centraliens, *n°621 du 25-10-2012, « Le point de vue des hommes de loi : propriété et usage des données », numéro spécial « L'Internet des Objets "IdO? Idéaux?" »: http://www.alain-bensoussan.com/internet-des-objets-propriete-et-usage-des-donnees/2012/11/15/*

(13) « Le réfrigérateur connecté, nouvelle cible des pirates informatiques » www.france24.com, Sébastien Seibt, 17-01-2014

(14) "The Internet of things is undoubtedly THE revolution of the 21st century*". (See French Senate, Information Report No. 784 dated 26-09-2012. Hearing of Eric Barbry, p.31).*

ERIC BARBRY

▪ L'internet des objets (IdO) est une technologie reposant sur l'interconnexion des objets entre eux. L'IdO crée un écosystème d'applications et de services intelligents destiné à améliorer et simplifier la vie des gens **(1)**. L'identification par radiofréquence (RFID) est un des éléments centraux, voire probablement le socle de l'internet des objets **(2)**. Par sa nature et son champ d'application infini, l'IdO soulève bien évidemment une série de questions juridiques, au premier rang desquelles la confidentialité des données.

▪ A ce jour, l'IdO ne fait pas l'objet d'une règlementation spécifique en Grèce, mais certaines technologies (géolocalisation et RFID) tombent clairement dans le champ de la mission attribuée à l'Autorité grecque de protection des données (ADAE) **(3)**. Le débat juridique est donc ouvert.

▪ Premièrement, concernant la RFID, l'ADAE a marqué son soutien à l'avis 5/2010 rendu par le groupe de travail « Article 29 » sur la proposition des entreprises relative au cadre d'évaluation de l'impact sur la protection des données et de la vie privée des applications reposant sur l'identification par radiofréquence (RFID) **(4)**. Dès 2007, l'ADAE avait d'ailleurs déjà dressé la liste des mesures de protection à mettre en œuvre par les entreprises utilisant la RFID, suggérant par exemple l'utilisation de technologies renforçant la vie privée, la mise en place de politiques de sécurité, l'obtention d'agrément par les responsables du traitement, l'application de contrôles d'accès, la tenue de registres de connexion, la mise en œuvre de systèmes de gestion de violation de données, ainsi que l'utilisation de technologies et de protocoles de cryptographie, d'anonymat, de non-association (impossibilité d'établir un lien entre deux actions déclenchées par un même utilisateur) et de non-observabilité (impossibilité de déterminer si une action est en cours de réalisation par un utilisateur donné).

▪ Deuxièmement, concernant la géolocalisation des personnes physiques (enfants, patients…), l'autorité hellénique s'est particulièrement intéressé au bouton « alarme » des GPS permettant de lancer un appel à l'aide, dans sa décision 112/2012. Cette fonction implique en effet la collecte, le traitement et le transfert hors UE/EEE de données personnelles sensibles (en particulier en cas de recours à la technologie *cloud*). Certes, cette décision est principalement axée sur les technologies GPS et GSM, toutefois les conclusions qu'elle tire en matière de finalités légitimes, d'information et de droits des personnes concernées, peuvent tout aussi bien s'appliquer aux technologies de l'IdO (puces RFID, codes barres, etc.). L'ADAE met particulièrement en exergue les obligations pesant sur les responsables du traitement, et notamment celle de fournir aux personnes des informations adéquates sur la collecte et le traitement des données les concernant et d'obtenir leur consentement le cas échéant, et celle de mettre en œuvre des mesures de sécurité organisationnelles et techniques pour protéger les données (cryptographie, mesures de sécurité physique, mécanismes d'authentification et d'identification, mots de passe de 8 caractères minimum). Cette même décision aborde également l'utilisation de systèmes de géolocalisation sur le lieu de travail et la vie privée des salariés.

▪ Troisième aspect de l'IdO abordé par l'autorité grecque: la technologie sans fil de machine à machine (M2M), et plus particulièrement l'« eCall » **(5).** Initié par l'Union européenne, l'eCall est système d'appels d'urgence embarqué permettant une intervention des services d'urgence plus rapide en cas d'accident de la route. L'appel d'urgence peut être déclenché soit manuellement par les occupants du véhicule, soit automatiquement par l'activation de détecteurs situés dans le véhicule. Lorsqu'il est activé, le système embarqué « eCall » établit une connexion vocale avec le 112 **(6)** directement avec le centre de réception des appels d'urgence, qui peut être une autorité publique ou un organisme privé agréé par un organisme public **(7)**.

▪ Enfin, bien qu'aucun texte législatif n'y fasse référence, les considérations de santé publique entourant à la mise en œuvre des technologies de l'IdO ne sont pas à négliger, et ont notamment été au centre du débat juridique sur la technologie RFID.

▪ En conclusion, alors les technologies de l'IdO pénètrent progressivement toutes les activités de la vie quotidienne, le législateur se retrouve confronté au défi d'instaurer un cadre juridique efficace et suffisamment protecteur de la sécurité et de la confidentialité des données permettant d'instaurer un climat de confiance, sans constituer un frein au développement de ces technologies.

REFERENCES

(1) European Commission, The Digital Agenda for Europe: http://ec.europa.eu/digital-agenda/en/internet-things

(2) Giovanni Buttarelli, Assistant European Data Protection Supervisor, "Internet of things: ubiquitous monitoring in space and time", European Privacy and Data Protection Commissioners' Conference Prague, Czech Republic, 29 April 2010, http://goo.gl/Aui573

(3) ADAE (Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών) www.adae.gr/en/

(4) Avis 5/2010 sur la proposition des entreprises relative au cadre d'évaluation de l'impact sur la protection des données et de la vie privée des applications reposant sur l'identification par radiofréquence (RFID) (http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp175_fr.pdf), tel que révisé par l'avis avis 9/2011, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp180_fr.pdf

(5) eCall: Time saved = lives saved

(6) Le 112 est le numéro d'appel d'urgence unique européen

(7) http://www.imobilitysupport.eu/imobility-support/its-deployment/ecall

GEORGE A. BALLAS
&
THEODORE
KONSTANTAKOPOULOS

- *The Internet of Things (IoT) is a technology and a market development based on the inter-connection of everyday objects among themselves and applications. The IoT enables an ecosystem of smart applications and services with an aim of improving and simplifying people's lives* ***(1)****. Radio-frequency identification (RFID) is a building block, probably "the key" component of the Internet of Things* ***(2)****. There are, however, due to nature and broad applicability of IoT, legal concerns around this technology and most importantly data privacy issues.*

- *While the implementation of IoT technologies has not, as of today, been officially regulated in Greece, geolocation and RFID technologies have been within the scope of the Hellenic Data Protection Authority's (DPA)* ***(3)*** *mission and work and an issue of legal debate.*

- *The DPA has adopted the WP29 Opinion 5/2010 on the Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications* ***(4)****. Even before its publishing, the DPA, in line with the WP29 Opinion 5/2010, in 2007 had listed the protection measures which should support the use of RFID technology, suggesting the use of Privacy Enhancing Technologies, Privacy and Security Policies, certification of the Data Processors, access controls, maintenance of activity logs, data breach management systems, the implementation of cryptographic technologies and protocols, anonymity, unlinkability and unobservability.*

- *Moreover, the DPA in its 112/2012 Decision addressed the issue of the use of geolocation technology for the localization of individuals (e.g. minors or patients) with the possibility of alarm release (help-button). Such technology may involve the collection and processing of sensitive personal data and data transfers outside the EU/EEA (especially in conjunction with the advancing use of cloud technology). Although the Decision focuses mainly on GPS and GSM technologies, its conclusions with regard to legitimate ground, information and Data Subject's rights could also apply to IoT technologies (RFID chips, barcodes, etc.). The DPA highlights in particular the Data Controller's obligation to provide adequate information to the Data Subjects about the data collection and processing in question (and obtain the Data Subject's informed consent, when required) and the Data Controller's obligation to implement appropriate organizational and technical data security measures, imposing e.g. the use of cryptography, physical security measures, verification and identification mechanisms and the use of 8 character passwords. Furthermore, the use of geolocation systems has been examined by the DPA with the context of privacy at workplace.*

- *The use of wireless machine to machine (M2M) technology has also been reviewed by the DPA within the context of "eCall" (in-vehicle emergency call)* ***(5)****, a European Union initiative, with the purpose to bring rapid assistance to motorists involved in a collision. "eCall" is an emergency call either generated manually by vehicle occupants or automatically via activation of in-vehicle sensors when an accident occurs. When activated, the in-vehicle "eCall" system establishes a 112-voice connection* ***(6)*** *directly with the relevant Public Safety Answering Point, which is a public authority or a private eCall centre that operates under the regulation and/or authorisation of a public body* ***(7)****.*

- *Finally, the public health considerations associated with the implementation of IoT technologies, though not included in any type of legislative text, have been a core element of the legal discussion on RFID technology.*

- *While the IoT technologies are being gradually "embedded" in most aspects of people's everyday activities, society and policy makers are faced with the challenge to create a climate for trust for this technology, combined with a legal framework addressing effectively the relevant questions of security and data privacy.*

REFERENCES

(1) *European Commission, The Digital Agenda for Europe:* http://ec.europa.eu/digital-agenda/en/internet-things

(2) Giovanni Buttarelli, Assistant European Data Protection Supervisor, "Internet of things: ubiquitous monitoring in space and time", European Privacy and Data Protection Commissioners' Conference Prague, Czech Republic, 29 April 2010, http://goo.gl/Aui573

(3) ADAE (Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών) www.adae.gr/en/

*(4) Opinion 5/2010 on the Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications (*http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp175_en.pdf*), as revised by Opinion 9/2011,* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp180_en.pdf

(5) eCall: Time saved = lives saved

(6) 112 is the single European emergency number

(7) http://www.imobilitysupport.eu/imobility-support/its-deployment/ecall

GEORGE A. BALLAS
&
THEODORE
KONSTANTAKOPOULOS

▪ Commentant la dernière édition du *Consumer Electronic Show* (« CES »), le plus grand salon high-tech du monde qui s'est tenu à Las Vegas au début du mois de janvier, le journal américain *The Washington Post* en est arrivé à la conclusion suivante : l'ère du PC est bel est bien révolue **(1)**. Son argument ? Il existe aujourd'hui un large éventail de produits qui se substituent aux ordinateurs et qui, même s'ils n'en remplissent pas encore toutes les fonctions, suffisent à satisfaire les besoins d'un utilisateur moyen.

▪ Certains de ces produits sont déjà disponibles sur le marché, ce sont les smartphones, les tablettes, les liseuses et les consoles de jeux connectés à Internet. Il ne s'agit cependant que de la partie émergée de l'iceberg : de nouvelles technologies sont en cours de développement, et vont considérablement changer non seulement la façon dont nous surfons sur le Web, mais également dont nous utilisons tous les objets qui nous entourent (appareils ménagers…). Chacun de ces objets offrira une variété d'usages, qui les rendront potentiellement beaucoup plus intrusifs que les simples gadgets auxquels ils peuvent ressembler de prime abord. Les très controversées « Google Glasses », les lunettes à réalité augmentée du géant américain de l'internet, seront (théoriquement) bientôt disponibles sur le marché, et d'autres fabricants travaillent sur des projets similaires. Ainsi, au CES, la société Intel a présenté Jarvis, une oreillette Bluetooth intelligente truffée de fonctionnalités, apparemment déjà présentes dans les Google Glass, et annoncé la sortie prochaine d'une montre intelligente et d'écouteurs intelligents. Selon les rumeurs, le coréen Samsung préparerait quant à lui la commercialisation d'un écran flexible, dont les différentes applications seront laissées à l'ingéniosité et à l'imagination des chefs de produits : ces écrans pourraient être installés sur les fenêtres d'une voiture, sur les portes de réfrigérateurs, sur des tasses…Bref, quasiment n'importe où.

▪ Tous ces produits, qui nous permettent de rester connectés où que nous soyons et où que nous allons, forment ensemble ce que l'on appelle « l'Internet des objets ». Des objets intelligents qui grâce à leurs fonctionnalités novatrices, vont nous aider au quotidien de multiples façon, mais qui, potentiellement, garderons trace de notre vie à chaque instant. A cet égard, de colossaux enjeux juridiques, cristallisés sur la protection de vie privée, se profilent à l'horizon. Notre capacité à relever les défis qui se présenteront passera nécessairement par l'analyse et la compréhension du fonctionnement technique de ces objets.

▪ L'autorité italienne de protection des données, le Garante **(2)**, a déjà abordé certaines des questions soulevées par les technologies actuelles de l'Internet des objets au regard du droit à la vie privée, et notamment par les smartphones. En effet, aujourd'hui, l'acteur clé de l'IdO est sans conteste le smartphone : notre téléphone nous permet de rester connectés 24 heures sur 24 et nous accompagne partout, il est à nos côtés dès notre réveil, nous suit sur notre lieu travail, et ne nous quitte même pas quand nous dormons. Aussi, nombre de questions se posent donc quant à l'utilisation des smartphones dans le cadre de l'IdO, et la prospection commerciale par téléphone en fait partie. Le code italien de protection des données encadre l'envoi de messages promotionnels sur les téléphones cellulaires et dispose que l'utilisation de SMS ou de courriers électroniques à des fins de prospection commerciale ne peut se faire qu'avec le consentement du propriétaire du téléphone. L'autorité italienne de protection des données a apporté plus de précisions sur ce point dans un règlement publié le 10 juin 2003 **(3)**. Par ailleurs, en 2011, le Garante a sanctionné une entreprise qui avait lancé une campagne de marketing par SMS sur des téléphones cellulaires, faute pour elle d'apporter la preuve qu'elle avait bien obtenu le consentement des personnes concernées pour procéder aux traitements de leurs numéros de téléphones. **(4)**. Par la suite, le Garante a procédé à des contrôles auprès de 14 sociétés spécialisées dans les campagnes de marketing direct par e-mail ou SMS, à l'issue desquels cinq d'entre elles ont écopé d'une amende de 300.000 € pour envoi de SMS sans consentement des personnes concernées **(5)**.

▪ Autre technologie phare de l'Internet des objets : la RFID. Aucune espèce n'est à signaler à ce jour en Italie, mais on peut souligner la publication par le Garante d'un document définissant les principes essentiels applicables en matière de RFID et donnant aux professionnels des orientations générales à suivre **(6)**. Enfin, s'agissant de l'IdO dans le secteur financier, le Garante a lancé, le 3 janvier 2014, un appel à contributions invitant les parties prenantes à lui faire part de leurs remarques ou expériences sur la gestion de la vie privée dans le cadre des paiements effectués sur des tablettes ou des smartphones, dans la perspective d'une recommandation qui devrait être adoptée prochainement **(7)**.

▪ Les objets de l'IdO restent assez rudimentaires, mais cela risque de changer très vite au vu du potentiel de développement des technologies. Les questions qui en déroulent promettent d'être extrêmement complexes : il suffit d'imaginer la possibilité de posséder, sur un même appareil, un accès Internet, un système de reconnaissance faciale et un GPS. Les professionnels du droit en général, et les avocats en particulier, doivent se préparer à ce bouleversement technologique et devenir de véritables experts techniques pour ne pas rater ce tournant juridique.

REFERENCES

(1) The PC is dead, and this year's CES proves it, Timothy B. Lee, 08-01-2014, www.washingtonpost.com

(2) Garante per la protezione dei dati personali, www.garanteprivacy.it/

(3) Sms promozionali o di vendita diretta: le regole per il corretto uso, Doc web 29836, 10-06-2003

(4) Campagne di marketing effettuate tramite numeri di cellulari: vietato l'invio di SMS promozionali senza il consenso degli interessati, Doc. web 1836396, 10-06-2011

(5) Marketing via sms o e-mail nel mirino del, Garante Newsletter N. 355, 27-01-2012

(6) "Etichette intelligenti" (Rfid): il Garante individua le garanzie per il loro uso, Doc web n.1109493 09-03-2005. Version anglaise disponible (Doc web 1121107)

(7) Avviso pubblico di avvio della consultazione su "Schema di provvedimento generale in materia di trattamento di dati personali nell'ambito dei servizi di mobile remote payment, Doc web 2830747, 12-12-2013

RAFFAELE ZALLONE

- *Commenting on the Consumer Electronic Show held in Las Vegas early this month, the Washington Post has come to the following conclusion: The PC is dead* ***(1)****. The point is that there is a wide range of products that are replacing PC's, even though they may not have all the functions of a PC but simply the functions an average user may need.*

- *Some of these products are already available on the marketplace: smartphones and tablets, book readers and gaming devices that have internet access. But this is only the tip of the iceberg: new technologies are being developed that will dramatically change the way we presently connect to the web; they will change the way we use our household products or other products. All of them will have a variety of use that makes these products potentially much more invasive than the simple gadgets they may seem. The much-tainted Google Glass will (apparently) be soon available on the marketplace, but other producers are working on similar products as well. At CES, Intel has introduced Jarvis, a smart headset with many of the capabilities apparently present in Google Glasses. They also announced a smart watch and smart earbuds. Samsung has been reported as working on a flexible screen, whose applications will be left to the ingenuity and the fantasy of product managers: they can be installed on car windows, on refrigerator doors, coffee mugs, practically anywhere.*

- *These products will all allow us to stay connected wherever we are and wherever we'll go; these products are what makes the Internet of Things: smart objects, devices, gadgets that will help us with their new, creative functions but that will potentially track our life in any given moment. There's no question that this shall definitely create new challenges under privacy laws, and the capability and the functions of each product needs to be fully understood to correctly address all the possible legal issues.*

- *The Italian Data Protection Authority* ***(2)*** *has already addressed at least some the issues of the Internet of Things under privacy law with respect to existing technologies. The most popular example of the devices that create the Internet of Things is by far the smartphone. It follows us anywhere, from our workplace to our bed when we sleep, and it allows us to stay connected 24/24 hours. The Italian Data Protection Code lays down the rules for using the cellular phone (hence the smartphone as well) to send promotional messages via SMS: the law states that use sms or e-mail for such purpose is allowed only with the consent of the owner of the phone. The Italian Data Protection Authority has specified the rules laid down in the Code in a regulation issued by the on June 10, 2003* ***(3)****. These rules have been constantly implemented: one of the most recent decisions on this point was laid down on June 11, 2011 against a company who had launched a marketing campaign via sms to cellular phones. The processing of the phone numbers to send the sms has been declared void, since there was no evidence of the consent of the subjects involved* ***(4)****. The Italian Data Protection Authority then has conducted an inspection on 14 companies specialized in direct marketing campaigns using either e-mail or sms: five such companies have been fined a total of 300.000 euro's for sending sms without due consent* ***(5)****.*

- *Another example of these technologies in the Internet of things is RFID's. Although there are no cases under Italian Law, the Authority on March 9, 2005, has published a detailed paper addressing the main issues with such technology and giving guidelines on the way to use it* ***(6)****. Finally, the Authority on January 3 this year has launched a call for comments and suggestion on a regulation aimed at addressing privacy issue with payments made via Tablets or Smartphones* ***(7)****.*

- *These products are quite simple, compared to the potential of the products on their way to be announced: the potential issues of having (just to make an example) face recognition, internet access and gps positioning on the same device are simply enormous. Therefore lawyers must be ready to understand any and all the functions and how they work if they want to be able to address all such potential legal issues.*

REFERENCES

(1) The PC is dead, and this year's CES proves it, Timothy B. Lee, 08-01-2014, www.washingtonpost.com

(2) Garante per la protezione dei dati personali, www.garanteprivacy.it/

(3) Sms promozionali o di vendita diretta: le regole per il corretto uso, Doc web 29836, 10-06-2003

(4) Campagne di marketing effettuate tramite numeri di cellulari: vietato l'invio di SMS promozionali senza il consenso degli interessati, Doc. web 1836396, 10-06-2011

(5) Marketing via sms o e-mail nel mirino del, Garante Newsletter N. 355, 27-01-2012

(6) "Etichette intelligenti" (Rfid): il Garante individua le garanzie per il loro uso, Doc web n.1109493 09-03-2005. Version anglaise disponible (Doc web 1121107)

(7) Avviso pubblico di avvio della consultazione su "Schema di provvedimento generale in materia di trattamento di dati personali nell'ambito dei servizi di mobile remote payment, Doc web 2830747, 12-12-2013

RAFFAELE ZALLONE

Qu'est-ce que l'Internet des objets (IdO) ?

▪ Le concept d'IdO est encore récent (2009), mais fait déjà l'objet de plusieurs définitions. Pour certains, cette expression fait référence à un ensemble d'« objets intelligents », d'« objets sociaux », ou d'« objets uniques identifiables dans une structure de type Internet », reflétant la fusion entre les objets (« things ») et le Web (Internet), et illustré par le dernier mot à la mode : « thingternet » **(1)**. Plus concrètement, l'IdO signifie que des objets ordinaires, tels que des baskets ou des réfrigérateurs, auront la possibilité de se connecter à l'Internet, via différentes technologies, comme le Bluetooth, la Wi-Fi et la RFID (tags et stickers).

▪ Tandis que l'évolution des technologies nous a fait passer des PC **(2)** à la tablette, en passant par les smartphones, l'Internet est quant à lui passé du « .com. » aux réseaux sociaux, pour arriver aujourd'hui à l'IdO. Sans en être conscients, nous croisons ces technologies tous les jours, lors d'activités diverses et variées : utiliser un service de localisation par GPS sur un smartphone, partager des informations sur les réseaux sociaux, rechercher en ligne la posologie d'un médicament, allumer le moteur d'une voiture, assurer l'identification et la traçabilité du bétail, vérifier la température d'un réfrigérateur, se connecter sur internet à partir d'un téléviseur, régler au télépéage, utiliser une pointeuse électronique au travail... **(3)**. Lorsque vous allez courir et que vous utilisez une application podomètre qui vous indique la distance parcourue et les calories dépensées, vous ne vous rendez probablement pas compte que ces actions sont suivies et détectées et que les informations qui s'y rapportent sont transmises sur Internet, à des fins diverses.

▪ Les avantages de l'IdO sont ainsi contrebalancés par les inconvénients qu'il pose en termes de sécurité et de confidentialité des données. Dans le monde entier, les acteurs économiques devraient donc prend à bras-le-corps les enjeux de l'IdO, et mettre en œuvre de mesures techniques nécessaires à la protection des données et de la vie privée en conformité avec la règlementation applicable dans chaque pays **(4).**

Le Mexique face à l'IdO

▪ Il a fallu près de 10 ans pour que le Mexique se dote d'une loi fédérale destinée à garantir la vie privée et la protection des données personnelles, répercutée dans le code civil fédéral, le code pénal fédéral ainsi qu'une série d'autres lois au niveau fédéral. C'est ainsi qu'en juillet 2010, le Congrès fédéral mexicain a adopté la loi fédérale sur la protection des données personnelles détenues par des particuliers (« LFPDPPP ») **(5)** après avoir procédé à la révision nécessaire des articles 6, 16 et 73 de la Constitution fédérale du Mexique. Depuis lors, sont considérés comme des droits constitutionnels fédéraux les droits d''accès, de rectification, d'annulation et d'opposition à l'égard des données personnelles, généralement désignés sous l'acronyme ARCO **(6)**.

▪ Aux termes de la LFPDPPP, les données à caractère personnel s'entendent de toute information relative à une personne, telles que son nom, sa date de naissance et son lieu de naissance, certaines d'entres elles ayant un caractère particulièrement sensible (données relatives à la santé, aux croyances religieuses, et aux préférences sexuelles). Ces informations ne peuvent être divulguées sans l'autorisation de la personne à laquelle elles se rapportent.

▪ L'Institut fédéral d'accès à l'information et à la protection des données (« IFAI ») **(7)** est l'autorité mexicaine en charge du respect de la réglementation en matière de protection des données. A ce titre, l'IFAI élabore régulièrement des lignes directrices sur des thèmes d'actualité touchant à l'informatique et aux libertés. Elle a ainsi publié des guides sur les mentions légales (article 16 et suivants de la LFPDPPP), les secrets commerciaux régis par le droit de la propriété industrielle **(8)**, l'utilisation de la photographie d'un individu fournie pour l'obtention d'un agrément délivré par l'administration **(9)**, les cas possibles de divulgation de la date de naissance d'un fonctionnaire **(10)**, ou encore la nature confidentielle du numéro d'identification national (CURP) attribué à chaque Mexicain **(11)**.

▪ En revanche, contrairement à ses homologues dans le monde, l'IFAI n'a pas encore émis de recommandation spécifique à l'égard des données recueillies par la RFID ou toutes technologies ou systèmes liés à l'IdO, ou concernant le traitement des données obtenues par ceux-ci.

▪ Il convient cependant de noter qu'en mai 2011, l'IFAI a signalé l'ouverture, à l'encontre des sociétés Sony Computer Entertainment et Sony Entertainment Network, d'une enquête officielle portant sur une faille de sécurité ayant affecté le réseau PlayStation au mois d'avril 2011 et la possible divulgation de données personnelles en résultant.

▪ Trois projets d'amendement à la LFPDPPP sont actuellement en discussion par le Congrès fédéral mexicain, mais la loi de protection des données personnelles étant très récente, le chemin sera encore long avant que le Mexique ne dispose d'un arsenal juridique complet lui permettant de faire face aux différents enjeux de l'IdO.

REFERENCES

(1) L'Internet des objets (IdO) est un concept informatique qui décrit un avenir où les objets physiques du quotidien seront connectés à l'Internet et seront en mesure de s'identifier auprès d'autres appareils « The Age of Thingternet: What is the Internet of Things? », www. iopedia.com)

(2) « PC boom is over as tablets and smartphones take over », Charles Arthur, www.theguardian.com, 30-08-2013.

(3) Cf. RFID Technology and Internet of Things, Dmitri Shiryaev, slideshare.net (2012), et Habrá 50 mil millones de objetos conectados a Internet en 2020 José Luis Becerra Pozas, 13-13-2013, computerworldmexico

(4) Cf. Study Looks at Risks of the Internet of Things , Bob Violino, baselinemag.com, 26-12-2013 ; et ¿Cómo protegerse en la era del Internet of Things?, Julio Vélez, 07-11-2013, altonivel.com.mx.

(5) Loi fédérale sur la protection des données personnelles détenues par des particuliers (LFPDPPP) et son Règlement d'application (RLFPDPPP)
(en espagnol)

(6) Derechos ARCO: Acceso, Rectificación, Cancelación, Oposición

(7) Autorité de protection des données mexicaine (IFAI)

(8) Secreto industrial o comercial. Supuestos de reserva y de confidencialidad (Criterio 13/13)

(9) La fotografía de una persona física que conste en su título o cédula profesional no es susceptible de clasificarse con carácter de confidencial, (Criterio 32/10)

(10) Casos en los que excepcionalmente puede hacerse del conocimiento público la fecha de nacimiento de los servidores públicos (Criterio 18/10)

(11) Clave Única de Registro de Población (CURP) es un dato personal confidencial (Criterio 3/10)

ENRIQUE OCHOA DE GONZÄLEZ ARGÜELLES

What is Internet of Things IoT?

- *Even though IoT is new concept (2009), there are several definitions for IoT. Some of said definitions refer to "smart objects", "objects getting social", "unique identifiable objects in an Internet like structure" and the new word "thingternet"* ***(1)****.*
- *In a nutshell, IoT refers to a scenario in which ordinary objects such as tennis shoes, refrigerators or others will have the capability to connect to the Internet. And this connection can be implemented by different kinds of technologies, including but not limited to Bluetooth, Wi Fi and Radio Frequency Identification (RFID) tags and stickers.*
- *While the evolution of technologies has taken us from the PC boom* ***(2)*** *to tablet, smartphones and other devices boom, Internet has taken us from the .com boom, through the social media boom and now to the IoT boom.*
- *In a common day, we get to see these technologies and probably do not realize its importance, potential and probable risks thereof. When you go for a run and use a device that allows you to measure the distance (pedometer), height (altimeter) and the burning of calories, when you use a GPS tracking device or a checking clock in your office, when you log into a service via a smartphone, TV or other device, etc. probably you are not fully aware that said actions are monitored and detected by different means and that the information therein is transmitted in the Internet for several purposes. Among others, you may find that people use these devices and technologies to: show an achievement in social media, to determine the intake of a medicine, to ignite a car, to track cattle, to display a location in social media, to measure the punctuality of employees, to find out if the temperature of a refrigerator is adequate, to know when to buy groceries, electronic toll devices, etc.* ***(3)***
- *Unfortunately, the use of the abovementioned technologies has a drawback which refers to the security of the information and the privacy of the data and said issue will have to be dealt in every company throughout the world by implementing technical measures and by complying with data protection and privacy laws and standards in each jurisdiction.* ***(4)***

Mexico facing IoT.

- *It took almost 10 years for Mexico to have a Federal Law to ensure privacy of individuals. The first efforts intended to modify the Federal Civil Code, the Federal Criminal Code and other laws. In July, 2010, the Mexican Federal Congress enacted the Federal Law for the Protection of Personal Data Held by Private Parties (Mexican Privacy Law)* ***(5)*** *after amending articles 6, 16 and 73 of the Mexican Constitution. As a consequence thereof, the rights for the access, rectification, cancellation and opposition to the use of personal data of individuals are now considered as federal constitutional rights (ARCO rights)* ***(6)****.*
- *Mexican Privacy Law sets forth that personal data includes information in relation to a person, such as name, date of birth, place of birth, and "sensitive information," which may include general health, religious beliefs, and sexual preferences. This information may not be disclosed without a person´s authorization.*
- *The Federal Institute for the Access to Public Information and Data Protection (IFAI)* ***(7)*** *is the Federal authority in Mexico regarding the enforcement of the Mexican Privacy Law and its Rules. IFAI has issued Guidelines for the drafting of the Privacy Notice (article 16 et al of the Mexican Privacy Law) and criterion regarding different topics, such as: confidential information of individuals and companies, including trade secrets regulated by the Industrial Property Law* ***(8)****; the photograph of an individual in a Professional License issued by the government* ***(9)****;cases in which the birth date of a public officer may be disclosed* ***(10)****; confidentiality of the Unique Key for the Population Registry (CURP) issued by the Ministry of State* ***(11)****.*
- *But not regarding specifically to data gathered by RFID or other devices and the treatment of said data by the companies that offer services referred to lines above.*
- *On May, 2011, IFAI issued an official communication by which it informed Sony Computer Entertainment and Sony Network Entertainment in Mexico about the initiation of an investigation regarding a breach of security in the PlayStation network in April 2011 and the possibility of personal data disclosed to third parties.*
- *Unlike its peers throughout the world, IFAI has not yet used an official communication regarding the use of RFID or other technologies.*

There are at least three drafts for the amendment of the Mexican Privacy Law that are now being discussed in the Federal Congress. Given that Mexico has had a law for the protection of privacy since 2014, there is still much work to do with the authorities in order to have a comprehensive legal framework in order to face the challenge of IoT.

.

REFERENCES

(1) The Internet of Things (IoT) is a computing concept that describes a future where everyday physical objects will be connected to the Internet and will be able to identify themselves to other devices. ("The Age of Thingternet: What is the Internet of Things?", www.iopedia.com)

(2) "PC boom is over as tablets and smartphones take over", Charles Arthur, www.theguardian.com, 30-08-2013.

(3) See RFID Technology and Internet of Things, Dmitri Shiryaev, slideshare.net; and Habrá 50 mil millones de objetos conectados a Internet en 2020, José Luis Becerra Pozas, 13-13-2013, computerworldmexico.

(4) See Study Looks at Risks of the Internet of Things , Bob Violino, baselinemag.com, 26-12-2013 ; and ¿Cómo protegerse en la era del Internet of Things?, Julio Vélez, 07-11-2013, altonivel.com.mx.

(5) Law on the Protection of Personal Data held by Private Parties (LFPDPPP) and its Rules (RLFPDPPP) (in Spanish)

(6) Derechos ARCO: Acceso, Rectificación, Cancelación, Oposición

(7) Mexican data protection authority (IFAI)

(8) Secreto industrial o comercial. Supuestos de reserva y de confidencialidad (Criterio 13/13)

(9) La fotografía de una persona física que conste en su título o cédula profesional no es susceptible de clasificarse con carácter de confidencial, (Criterio 32/10)

(10) Casos en los que excepcionalmente puede hacerse del conocimiento público la fecha de nacimiento de los servidores públicos (Criterio 18/10)

(11) Clave Única de Registro de Población (CURP) es un dato personal confidencial (Criterio 3/10)

ENRIQUE OCHOA DE GONZÁLEZ ARGÜELLES

PAYS / COUNTRY	CABINET / FIRM	CONTACT	TELEPHONE	EMAIL
Afrique du Sud *South Africa*	Michalsons Attorneys	Lance Michalson John Giles	+27 (0) 21 300 1070	lance@michalsons.co.za john@michalsons.co.za
Allemagne *Germany*	Schulte Riesenkampff	Tim Caesar	+49 (69) 900 26 876	tim.caesar@schulte-lawyers.com
Angleterre *UK*	Preiskel & Co LLP	Danny Preiskel	+ 44 (0) 20 7332 5640	dpreiskel@preiskel.com
Argentine *Argentina*	Estudio Millé	Antonio Millé Rosario Millé	+ 54 11 5297 7000	antonio@mille.com.ar rosario@mille.com.ar
Belgique *Belgium*	Philippe & Partners	Jean-François Henrotte	+ 32 4 229 20 10	jfhenrotte@philippelaw.eu
Brésil *Brazil*	Melchior, Micheletti e Amendoeira Advogados	Silvia Regina Barbuy Melchior	+ 55 113 8451511	melchior@mmalaw.com.br
Canada *Canada*	Langlois Kronström Desjardins	Jean-François De Rico	+1 418 650 7923	jean-francois.derico@lkd.ca
Chine *China*	Jade & Fountain PRC Lawyers	Jun Yang	+86 21 6235 1488	jun.yang@jadefountain.com
Colombie *Colombia*	Marrugo Rivera & Asociados	Ivan Dario Marrugo Jimenez	+57 1 4760798	imarrugo@marrugorivera.com
Espagne *Spain*	Lexing Spain	Marc Gallardo	+ 34 93 476 40 48	marc.gallardo@lexing.es
Etats-Unis *USA*	IT Law Group	Françoise Gilbert	+ 1 (650) 804 1235	fgilbert@itlawgroup.com
France *France*	Alain Bensoussan-Avocats	Alain Bensoussan	+33 1 82 73 05 05	paris@alain-bensoussan.com
Grèce *Greece*	Ballas, Pelecanos & Associates L.P.C.	George A. Ballas	+ 30 210 36 25 943	central@balpel.gr
Israël *Israel*	Livnat, Mayer & Co.	Russell D. Mayer	+972 2 679 9533	mayer@lmf.co.il
Italie *Italy*	Studio Legale Zallone	Raffaele Zallone	+ 39 (0) 229 01 35 83	r.zallone@studiozallone.it
Liban *Lebanon*	Kouatly & Associates	Rayan Kouatly	+ 961 175 17 77	info@kouatlylaw.com
Luxembourg *Luxembourg*	Philippe & Partners	Jean-François Henrotte	+ 32 4 229 20 10	jfhenrotte@philippelaw.eu
Maroc *Morocco*	Bassamat & Associés Zineb Laraqui	Bassamat Fassi-Fihri Zineb Laraqui	+ 212 522 26 68 03 + 212 66 144 8284	contact@cabinetbassanat.com zlaraqui@zineblaraqui.com
Mexique *Mexico*	Langlet, Carpio y Asociados, S.C.	Enrique Ochoa De Gonzälez Argüelles	+ 52 55 25 91 1070	eochoa@lclaw.com.mx
Norvège *Norway*	Føyen Advøkatfirma DA	Arve Føyen	+ 47 21 93 10 00	arve.foyen@foyen.no
Suisse *Switzerland*	Sébastien Fanti	Sébastien Fanti	+ 41 (0) 27 322 15 15	sebastien.fanti@sebastienfanti.ch
Tunisie *Tunisia*	Younsi & Younsi International Law Firm	Yassine Younsi	+216 71 34 65 64	cabinetyounsi_younsi@yahoo.fr

La JTIT est éditée par Alain Bensoussan Selas, société d'exercice libéral par actions simplifiée, 58 boulevard Gouvion-Saint-Cyr, 75017 Paris, président : Alain Bensoussan
Directeur de la publication : Alain Bensoussan – Responsable de la rédaction : Isabelle Pottier
Diffusée uniquement par voie électronique – gratuit –
Abonnement à partir du site : Abonnement à partir du site : http://www.alain-bensoussan.com/outils/abonnement-petit-dejeuner-juristendance/
ISSN 1634-0701