Chronique du droit des nouvelles technologies

L'« Internet of Things » : une nouvelle brèche dans la vie privée et la protection des données à caractère personnel

Toute entreprise, grande ou petite, dépend de l'informatique, domaine sujet à un renouvellement constant. Ces nouveautés techniques entraînent inévitablement de nouvelles questions juridiques impactant le quotidien des salariés et des employeurs. La présente rubrique, à paraître tous les mois, a pour objectif de couvrir les sujets d'actualité et les évolutions en droit des nouvelles technologies au niveau de la législation luxembourgeoise et européenne.

Apparu au cours de l'année 2008, le Web 3.0 – également connu sous le nom de l'«Internet des objets» ou de l'«Internet of Things» – se veut être la dernière évolution en date du réseau des réseaux. Cette appellation qui peut faire peur de prime abord désigne en fait le phénomène d'apparition de plus en plus massive d'objets «intelligents» et «connectés», capables de collecter, de traiter et de transmettre via les réseaux des informations relatives à l'environnement dans lequel ils se trouvent.

Du logiciel tournant sur un smartphone et comptabilisant le nombre de pas réalisés par jour par le propriétaire dudit téléphone, au frigo de la ménagère passant automatiquement commande dans le magasin du coin lorsque les vivres viennent à manquer, en passant par les lunettes intelligentes dernièrement développées par le géant Internet de Silicon Valley, les exemples d'application de l'Internet of Things (ci-après «IoT») ne manquent guère. Ceux-ci ne constituent pourtant qu'une infime partie d'un phénomène au potentiel indéfini, que d'aucuns oseront comparer au phénomène de l'avènement de l'Internet lui-même en terme d'importance. Rappelons-nous, apparu il y a une dizaine d'années seulement, ce dernier a aujourd'hui changé nos vies.

Il est certes vrai que l'IoT constitue une invention qui permettra sans doute de résoudre bien des problèmes contemporains. Gestion des besoins vitaux pour l'humanité, gestion de l'approvisionnement alimentaire, maîtrise de la pollution dans les grandes villes, maîtrise des coûts de la santé par l'instauration d'une médecine préventive ou encore l'optimisation des réseaux des distributions d'énergie sont autant d'exemples d'application de l'IoT qui sont et qui seront bénéfiques à toutes et à tous.

Le développement rapide que connaît l'IoT aujourd'hui est sans doute dû à la présence de plusieurs facteurs techniques réunis. Ainsi, l'arrivée de l'Internet Protocol Version 6 (l'IPV6), la miniaturisation des capteurs et la baisse de leurs coûts, le développement des technologies «BigData» et l'arrivée des réseaux de communications très haut débit constituent sans aucun doute un terraux fertile à l'avènement de l'IoT.

À côté des avancées majeures qu'il représente, force est malheureusement de constater que le Web 3.0 soulève également une multitude d'interrogations sur le plan juridique, principalement en termes de vie privée et de respect des données à caractère personnel. Ces risques ont été rappelés par le Groupe de Travail Article 29 (ci-après, le «Groupe Article 29»), le 16 septembre dernier, dans son Opinion 8/2014 on the Recent Developments on the Internet of Things (ci-après, «l'Opinion 8/2014») (1.). Bien que les documents émanant de cet organisme ne soient pas légalement contraignants, ils demeurent néanmoins d'une importance capitale en pratique, dès lors qu'ils reflètent les avis des différents représentants de chacune des autorités nationales pour la protection des données à caractère personnel. L'Opinion 8/2014 est également importante en ce qu'elle précise la manière d'appliquer les traditionnels principes du droit européen de la protection des données à caractère personnel au contexte spécifique de l'IoT (2.).

Une problématique similaire à l'IoT est celle du développement des nouveaux compteurs intelligents d'énergie: le «smart metering» ou le «smart grid». Ces compteurs disposent d'une technologie avancée leur permettant d'identifier et d'enregistrer, en temps réel, la consommation en énergie d'un ménage spécifique. Ceci permet par exemple aux fournisseurs d'énergie d'optimiser la distribution d'énergie, ou de proposer des offres personnalisées à leurs clients.

Consciente des risques qu'une telle pratique peut avoir sur la vie privée, la Commission européenne s'est également penchée sur la question. Ainsi, dans sa Recommandation du 10 octobre 2014 (ci-après, la «Recommandation»), elle enjoint les États membres de mettre en place un modèle d'analyse d'impact sur la protection des données des réseaux intelligents et des systèmes intelligents de mesure (3.). Cette procédure a été dûment suivie lorsque la CNPD, l'autorité nationale luxembourgeoise, a participé dans l'analyse d'impact du projet de smart metering de Luxmetering. Bien que ces documents voient le jour au niveau européen, ils ne resteront pas sans conséquence sur le plan du droit luxembourgeois.

1. Des risques amplifiés associés à l'avènement de l'IoT

Dans son Opinion 8/2014, le Groupe Article 29 dénonce l'amplification des risques d'atteinte à la vie privée et aux données à caractère personnel concernant l'information traitée par les «appareils intelligents» dans le cadre de l'IoT.

Le Groupe Article 29 pointe tout d'abord le manque de contrôle que l'utilisateur à sur ses données, ainsi que l'asymétrie d'information qui existe entre l'utilisateur et le vendeur de l'appareil intelligent quant à la question de savoir si des données sont traitées et si oui, quelles sont les données traitées. Ceci a pour conséquence que la qualité du consentement au traitement de ses données donné par la personne concernée, en principe nécessaire pour pouvoir effectuer un traitement de données, peut laisser à désirer. N'ayant pas connaissance de toutes les données traitées, l'utilisateur ne peut en effet donner validement son consentement.

Le Groupe Article 29 souligne également le fait que l'IoT permet de croiser plus aisément des données, ce qui peut aboutir à l'obtention de données ayant un caractère davantage sensible que les données originales qui ont été croisées. Un tel traitement de données sensibles est en principe interdit en droit luxembourgeois. Ce croisement de données peut également mener à des pratiques de profilage des personnes concernées. Enfin, des risques amplifiés de sécurité des données récoltées dans le cadre de l'IoT sont également pointés du doigt par le Groupe Article 29, dès lors que les données transitent sur des appareils «intelligents», dont les capacités d'encryptions et de sécurisation de l'information sont bien souvent limitées.

2. L'application de la législation protectrice des données à caractère personnel aux traitements de données dans le cadre de l'IoT

De manière générale, le droit européen de la protection des données – à savoir, le droit national de chaque État membre, tel qu'harmonisé par la Directive 95/46/CE – régule la question des traitements de données à caractère personnel des citoyens européens.

Dans son Opinion 8/2014, le Groupe Article 29 rappelle que cette loi a vocation à s'appliquer pour tout traitement réalisé dans le cadre des activités d'un établissement fixe du responsable du traitement – la personne qui définit les moyens et les finalités du traitement – établi sur le territoire d'un État membre. Elle s'applique également lorsque ledit responsable n'est pas établi sur le territoire d'un État membre, mais que celui-ci traite tout de même des données en utilisant des «équipements» situés sur le territoire d'un État membre. Le Groupe Article 29 précise à cet égard que tout «smart device» traitant des données dans le cadre de l'IoT doit être considéré comme un tel «équipement», si bien que les législations nationales en matière de protection des données à caractère personnel de l'État sur lequel l'équipement est situé doivent trouver à s'appliquer.

Les obligations en matière de protection des données que prévoient ces législations nationales incombent principalement aux responsables de traitement. À cet égard, le Groupe Article 29 livre d'intéressantes précisions sur la question de la personne à qui revient la qualité de responsable de traitement parmi les différents acteurs de l'IoT. Ainsi, le responsable du traitement sera tantôt le fabricant d'appareils intelligents, tantôt le développeur d'applications tournant sur ces appareils, tantôt encore le responsable de la plateforme sociale interagissant avec les appareils intelligents.

Afin d'aider ces responsables du traitement à observer les obligations leur incombant en vertu de la protection des données à caractère personnel, le Groupe Article 29 a également énoncé une série de recommandations. Parmi celles-ci, les plus signifiantes sont la mise en place d'un système de «privacy by design», la réalisation d'une analyse d'impacts avant la mise sur le marché d'applications tournant dans l'IoT, l'effacement des «données brutes» dès qu'elles ne sont plus nécessaires, le fait de donner aux personnes concernées le plus de contrôle possible sur leurs données, le fait de les informer de manière régulière du fait que leurs données sont collectées par les appareils intelligents, ou encore le fait de fournir aux personnes concernées des outils leur permettant de lire et d'éditer leurs propres données avant qu'elles ne soient traitées.

Bien que l'Opinion 8/2014 n'ait pas force de loi et ne constitue qu'un document consultatif, celle-ci ne sera néanmoins pas sans conséquence sur le plan luxembourgeois. En effet, les opinions du Groupe Article 29 représentent l'avis de l'ensemble des représentants des autorités nationales pour la protection des données à caractère personnel des États membres de l'Union européenne. Partant, la Commission nationale pour la protection des données (ci-après, la «CNPD») en tiendra certainement compte dans la manière dont elle appliquera et interprétera la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel (ci-après, la "Loi luxembourgeoise sur la protection des données") dans le cadre de l'IoT. Celle-ci sera a priori d'application chaque fois qu'un smart device se trouvant sur le territoire luxembourgeois traite des données à caractère personnel.

Cela aura pour conséquence que le responsable du traitement – identifié par l'Opinion 8/2014 comme étant, selon le cas, le fabriquant de l'appareil intelligent, voire le développeur de l'application tournant sur celui-ci, voire le responsable de la plateforme sociale sur laquelle les données sont publiées – sera tenu de respecter les obligations lui incombant en vertu de cette loi.

Parmi celles-ci, l'on citera particulièrement l'obligation de respecter les principes de qualité des données, l'obligation de réaliser les notifications nécessaires auprès de la CNPD et l'obligation de respecter les droits à l'information et à la rectification des personnes concernées. Il est également à noter qu'en vertu de la Loi luxembourgeoise sur la protection des données, les transferts de données vers des États tiers ne présentant pas un niveau de protection adéquat ne peuvent avoir lieu que moyennant le respect de certaines conditions. Il est important de signaler que l'IoT impliquera bien souvent pour le responsable du traitement le respect d'une obligation supplémentaire. En effet, dès lors que le responsable du traitement – par exemple, le fabriquant d'un smartphone – ne disposera bien souvent pas d'un établissement au Luxembourg, celui-ci sera tenu de désigner un représentant local chargé du respect des obligations mises en place par la Loi luxembourgeoise sur la protection des données. Il convient enfin de rappeler que l'IoT impliquera souvent le traitement de données à caractère sensible, ce qui est en principe interdit en droit luxembourgeois.

3. La Recommandation de la Commission sur le Smart Metering

Problématique fortement liée à celle de l'IoT, le smart metering et le smart grid posent également un certain nombre de questions en matière de protection des données à caractère personnel, dès lors que ces types de dispositifs permettent de récolter des données à caractère personnel – potentiellement de nature sensible – concernant par exemple les habitudes de consommation d'énergie des utilisateurs des réseaux, leur style de vie ou encore les périodes auxquelles ils sont présents à la maison.

Afin de prévenir les atteintes à la vie privée, ou du moins, de les diminuer, la Commission européenne a récemment pris la Recommandation du 10 octobre 2014 concernant le modèle d'analyse d'impact sur la protection des données des réseaux intelligents et des systèmes intelligents de mesure. Celle-ci encourage les États membres à prévoir l'utilisation du modèle d'analyse d'impact sur la protection des données (ci-après, «AIPD») en cas de mise en place d'un système de smart metering sur leur territoire. Ce modèle d'analyse d'impact a été mis au point par la Commission et est disponible sur le site Internet de la task-force «Réseaux intelligents». Il a en outre fait l'objet d'une étude de la part du Groupe Article 29. Celle-ci a donné naissance à l'Opinion 7/2013 du Groupe Article 29. Partant, la Commission recommande également aux États membres et aux responsables des réseaux électriques intelligents de tenir compte des observations réalisées par le Groupe Article 29 dans cette opinion.

Tout comme en matière d'IoT, la Recommandation et le modèle d'AIPD encouragent fermement la mise en place d'un système de «privacy by design». La Recommandation incite également les responsables du traitement à prendre les mesures techniques et organisationnelles appropriées pour assurer la protection des données à caractère personnel.

Dans son modèle d'AIPD, la Commission fournit également un «step plan» afin de réaliser l'analyse d'impact préconisée. Par exemple, la Commission recommande, avant toute chose, de réaliser une analyse préalable, consistant à déterminer si une AIPD complète est effectivement nécessaire. Dans l'affirmative, la Commission recommande alors de lancer une phase d'initiation, afin d'organiser de manière pratique l'AIPD. S'en suivra une description du système de réseau intelligents et une analyse des risques qu'il produit en matière de protection des données à caractère personnel. Une fois ceux-ci identifiés, un rapport sera rédigé afin de rendre compte de l'AIPD effectuée et des conclusions à en tirer.

Il est à noter que le Luxembourg a – une fois de plus – été un des avant-coureurs en la matière. Ainsi, une analyse d'impact sur la mise en place d'un système de compteurs intelligents sur le territoire du Luxembourg par le groupement d'intérêt économique Luxmetering est en cours de réalisation, en collaboration avec la CNPD. Le Luxembourg se positionne donc en bon élève de classe, dès lors que la réalisation d'une telle analyse d'impact n'est à ce jour pas obligatoire. Elle le deviendra néanmoins – dans certaines conditions – lorsque le nouveau règlement européen sur la protection des données à caractère personnel aura vu le jour.

Vincent WELLENS (cf. portrait)
Avocat à la Cour
Partner chez NautaDutilh Avocats Luxembourg S.à r.l.
vincent.wellens@nautadutilh.com

Nicolas RASE
Associate chez NautaDutilh Avocats Luxembourg S.à r.l.
nicolas.rase@nautadutilh.com
www.nautadutilh.com

Création de Fedil - ICT asbl

A l'issue de son assemblée générale constituante l'association Fedil – ICT a été officiellement créée le 13 octobre 2014 pour remplacer le groupe de travail du même nom qui opérait au sein de l'organisation patronale depuis plus d'une décennie.

Lors de l'assemblée, Robert Dennewald et Gérard Hoffmann, respectivement président et administrateur de la Fedil Business Federation Luxembourg ont présenté le bilan des activités de Fedil-ICT. Ils ont rappelé le rôle primordial joué par la Fedil pour dynamiser la compétitivité du marché ICT et média au Luxembourg et lui prodiguer une stature internationale.

Lors de la création d'ICTluxembourg, organisation faîtière regroupant les principales associations actives dans le secteur ICT dont FEDIL-ICT, Fedil a décidé de convertir son groupe de travail vers la forme associative pour y regrouper les membres de la Fedil actifs dans le secteur ICT au sein d'ICTluxembourg. C'est surtout le besoin de servir l'intérêt de ses membres qui a poussé la Fedil à faire le pas pour canaliser les efforts du secteur en vue d'assurer au mieux sa représentativité.

Le secteur ICT est un des principaux piliers de l'économie luxembourgeoise et représente près de 7% du PIB et compte à son actif non loin de 15000 emplois hautement qualifiés. Les 80 membres ICT/Media de la Fedil totalisent à eux seuls autour des 70% du PIB du secteur. C'est donc autour de ses membres que vont se cristalliser les activités de cet acteur de poids au Luxembourg. Fedil – ICT asbl entend contribuer de manière substantielle aux travaux d'ICTluxembourg et dans l'intérêt de l'ensemble du secteur.

Ces travaux seront en grande partie orientés par les initiatives gouvernementales dans le cadre de la stratégie nationale Digitallëtzebuerg et auxquelles le secteur privé souhaite s'associer. A côté de sa contribution à ICTluxembourg, Fedil – ICT poursuivra la mission que ses membres lui auront confiée et qui s'articulera autour du marché unique numérique et des missions d'étude.

Les 36 membres fondateurs ont alors élu à l'unanimité le conseil d'administration de Fedil – ICT asbl et approuvé le budget de l'association. Ont été nommés administrateurs:
Daniel Biedermann SES S.A. ;
Amal Choury eKenz S.A. , Vice-présidente ;
Yves Elsen Hitec Luxembourg S.A. ;
Gérard Hoffmann Telindus S.A. , Président ;
Olivier Lemaire Ernst Young S.A. ;
Edith Magyarics Victor Buck Services S.A. ;
Marcel Origer LuxConnect S.A. ;
Jean-Marie Spaus POST Telecom ;
Tun Van Rijswijk Broadcasting Center Europe S.A..

Nima Azarmgin a été nommé secrétaire général de l'association.

Le conseil d'administration se réunira une première fois début décembre pour élaborer son plan d'action.