Image not found or type unknown

Objets connectés et données personnelles

publié le **01/10/2014**, vu **4409 fois**, Auteur : Murielle Cahen

Le télécran, objet fictif inventé par George Orwell dans son roman 1984, qui permet à la fois de diffuser des messages de propagande du Parti mais également permettant à la Police de la Pensée d'entendre et de voir ce qui se fait dans chaque pièce où s'en trouve un individu, n'est plus si éloigné de la réalité. Les objets qui nous entourent sont de plus en plus connectés et les entreprises collectent par ce biais de plus en plus de données quantifiées sur les utilisateurs. L'explosion de « l'Internet des objets » pose des questions sur l'utilisation et la protection des informations personnelles contenues dans ces objets connectés.

L'ère du « tout-connecté » n'est plus si hypothétique. Dans une affaire récente, un concepteur anglais de logiciels, DoctorBeet, a mis en évidence sur son blog le fait qu'un téléviseur LG espionnait les téléspectateurs. La nouvelle a fait le tour du monde.

DoctorBeet avait remarqué que des publicités s'affichaient sur son téléviseur et que ce dernier enregistrait son comportement à son insu. Après avoir désactivé l'option de collecte de données activée par défaut, il s'est aperçu que l'envoi des données se poursuivait tout de même permettant même la collecte des fichiers présents sur une clé USB qui avait été branchée sur le téléviseur !

L'entreprise LG s'est finalement excusée sous le poids de la pression médiatique et a promis une mise à jour du logiciel. Cette nouvelle ère est une véritable révolution. D'ici 2020, plus de 80 milliards de produits seront ainsi connectés à Internet : ordinateurs connectés ainsi que toutes les variantes de ces derniers, Smartphones, tablettes…

Et également de nombreux *smart* objets : TV, frigidaires, voitures, montres, chaussures, lunettes, valises, pèse-personnes, machines à laver, consoles de jeu, stylos, aspirateurs… Ainsi, en 2018, chaque personne possèdera huit objets connectés en moyenne. Le géant Google a déjà créé de nombreux objets tels que les Google Glass, la Google car ou encore les lentilles de contact permettant de mesurer le taux de diabète. Mais ce dernier ne compte pas s'arrêter là et pourrait créer des lentilles de contact nous permettant d'enregistrer et de sauvegarder notre vie quotidienne. La connexion des objets apporte une « expérience client », une personnalisation de cette relation à l'extrême.

Les objets connectés sont intelligents et peuvent se connecter entre eux. Les données personnelles sont envoyées aux entreprises qui peuvent ainsi mieux connaître leurs clients. Même notre corps va devenir connecté via l'utilisation de capteurs corporels connectés – bracelets, podomètres, balances, tensiomètres –, et d'applications mobiles. Véritable révolution pour certains, pratique marginale pour d'autres, le sujet est complexe à aborder en raison de l'hétérogénéité des pratiques de « *quantified self* », de la diversité des outils et applications concernés, de leurs caractéristiques et de leurs fonctionnalités. Ainsi, se pose la question : peut-on continuer à protéger nos données personnelles avec l'invasion des objets connectés ?

I- Les risques juridiques relatifs à l'utilisation de ces objets connectés

A) Une surveillance clandestine

L'affaire du téléviseur LG révèle une certaine surveillance clandestine. Le pouvoir potentiel de ces objets dits intelligents sur notre vie quotidienne inquiète car il s'apparente à une forme d'espionnage domestique. En effet, si un tel appareil est connecté à Internet, il est possible de le trouver et de le surveiller grâce à des moteurs de recherches.

Il devient alors assez simple pour des pirates de les détourner de leur fonction première. De plus, s'ils ont la faculté d'apprendre à se gérer de manière autonome et en fonction de notre comportement, ils pourront bientôt développer des fonctionnalités différentes de celles initialement prévues. Le marché des objets connectés a vocation à devenir un immense terrain de jeu pour des cybercriminels ou des agences gouvernementales mal intentionnées : ils pourraient contrôler à distance tous les appareils connectés de notre domicile.

En 2013, des experts informatiques ont démontré qu'il était possible de désactiver à distance les freins d'une voiture électrique. La dangerosité de l'utilisation de ces appareils tient principalement dans la quantité et la variété des informations personnelles qu'ils permettent de recueillir, ainsi que la géolocalisation des personnes et des objets mêmes. L'ensemble de ces données permet de connaître environ tout de notre vie. La surveillance est alors totale. Or, une grande partie des consommateurs ne perçoivent pas toujours les difficultés de ces évolutions technologiques. Selon un sondage publié par Havas Media France en janvier 2014, près de 60% des internautes voient la généralisation des objets connectés d'ici 5 ans, car ils sont source de progrès (75%) et facilitent la vie (71%).

B) Un traitement des données personnelles

Copyright © 2024 Légavox.fr - Tous droits réservés

Le traitement des données personnelles est d'autant plus important qu'il peut concerner des données sensibles de santé. L'ampleur des « *quantified self* », ces petits objets qui mesurent la température de notre corps ou notre rythme cardiaque, repose selon la CNIL sur la collecte et le traitement de données dites « sensibles » qui, à cet égard, doivent faire l'objet d'une protection renforcée. Le caractère sensible de ces données tient à leur communication à des tiers, tels que les assureurs par exemple. De plus, d'autres données qui ne sont pas classées « sensibles » doivent faire l'objet d'une vive attention.

Il s'agit notamment des données de géolocalisation des individus. En effet, de nombreuses applications permettent de savoir où se situe exactement un individu. Si ces données viennent à être détournées, elles pourraient être très utiles aux cybercriminels ou autres personnes malveillantes. La géolocalisation fait l'objet de toutes les craintes, craintes alimentées par la loi relative à la géolocalisation du 28 mars 2014.

Cette loi prévoit que dans le cadre d'une enquête et sous l'autorité d'un juge, les enquêteurs peuvent avoir recours à « tout moyen technique destiné à la localisation en temps réel » d'une personne, « d'un véhicule ou de tout autre objet ». Pour garantir le développement du marché des objets connectés, il devient nécessaire d'assurer aux individus le respect de leurs droits et ainsi de rassurer le consommateur. Les industriels ne doivent donc pas faire l'impasse sur la sécurité du produit dès la conception. De plus, conformément à l'article 226-17 du Code pénal, le non-respect de l'obligation de sécurité imposée à tout traitement de données à caractère personnel est sanctionné de 5 ans d'emprisonnement et de 300 000 € d'amende. Lorsque c'est une personne morale qui est en cause, l'amende peut être multipliée par 5 et atteindre jusqu'à 1 500 000 €.

II- La protection juridique relative à l'utilisation de ces objets connectés

A) Le contrôle de la CNIL

Dès 2009, la CNIL a publié une communication sur l'internet des objets. Elle y exposait les perspectives et les enjeux du développement de ce secteur extraordinaire, tout en soulignant que cette avancée ne devait pas se réaliser au détriment de la vie privée et de la protection des données personnelles.

Copyright © 2024 Légavox.fr - Tous droits réservés

Un avis du groupe des CNIL européennes dit G29 est maintenant attendu sur le sujet. En Europe comme en France, les données personnes sont protégées par la loi. Leur utilisation est soumise à la loi Informatique et Libertés et à la directive du 24 octobre 1995 sur la protection des données personnelles. Constitue une donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. Les données sensibles telles les données de santé sont encore plus protégées.

Cependant, la loi Informatique et Libertés offre une protection réduite si la personne a consenti car le consentement est au cœur du dispositif légal. Par principe, un traitement de données à caractère personnel est licite s'il a reçu le consentement de la personne concernée. Ce système est le système de l'opt in. Or, le consentement ne sera plus obligatoire lorsque le traitement est nécessaire à l'exécution d'un contrat. Le législateur présume que la personne a implicitement consenti au traitement des données la concernant dès qu'elle contracte.

A titre d'exemple, lorsqu'une personne s'inscrit sur un réseau social tel que *Facebook* ou *Twitter* , elle fournit des données personnelles lors de son inscription. Si la personne souhaite s'inscrire sur le réseau, elle n'a pas le choix. Si elle ne veut pas voir ses données collectées, la seule solution est de renoncer au bénéficie de l'utilisation que lui procure le service ou le produit. Cependant, le responsable du traitement devra respecter de son côté les principes imposés par la loi (proportionnalité, pertinence, durée et finalité) ainsi que l'obligation déclarative à la CNIL ou la demande d'autorisation pour les traitements les plus graves.

Le système va certainement devoir évoluer afin de repenser les nouveaux enjeux qu'implique cette *hyperconnectivité*. Des difficultés apparaissent notamment concernant le droit effectif d'opposition lorsque le constructeur n'est pas européen mais chinois ou coréen, et concernant le droit de regard des puces par les utilisateurs. Laure Marino, Professeur à l'Université de Strasbourg, propose de lancer une réflexion sur une éventuelle procédure alternative de règlements des litiges à l'image de celles créées pour les conflits entre les titulaires de marques et les titulaires de noms de domaine. En effet, cette procédure permet de régler les litiges plus rapidement, plus efficacement et à moindre cout.

B) Les recommandations de la CNIL

L'émergence des objets connectés questionne le cadre juridique actuel notamment sur la définition de la donnée de santé ou de la responsabilité dans le cadre du partage automatisé des données. En consacrant le numéro 2 des Cahiers Innovation et Prospective au sujet du « quantified self » et des objets connectés, la CNIL adopte une démarche pragmatique pour proposer une analyse profonde de l'impact potentiel de ces nouvelles pratiques sur la vie privée et les libertés individuelles. La CNIL donne ainsi les recommandations suivantes :

- utiliser, si possible, un pseudonyme pour partager les données ;

Copyright © 2024 Légavox.fr - Tous droits réservés

- ne pas automatiser le partage des données vers d'autres services (notamment vers les réseaux sociaux) ;

- ne publier les données qu'en direction de cercles de confiance ;

- effacer ou récupérer les données lorsqu'un service n'est plus utilisé.

Elle met en garde les utilisateurs sur la prolifération de leurs données via les réseaux sociaux et rappelle que la frontière peut être floue entre le médical et le simple suivi de son bien-être. Une donnée qui peut sembler à priori anodine pour un utilisateur au moment où il la partage peut en fait recéler beaucoup d'informations pour un spécialiste qui pourrait y avoir accès par la suite et l'utiliser à des fins de ciblage ou de profilage.

-

Sources :

- http://www.village-justice.com/articles/Objets-connectes-challenge-des,17186.html

- http://www.lesnumeriques.com/objets-connectes-securite-donnees-a1790.html

- http://www.lemonde.fr/economie/article/2014/02/17/objets-connectes-attention-au-precipice_4367698_3234.html

- http://www.net-iris.fr/veille-juridique/actualite/33144/nouveaux-objets-connectes-et-protection-des-donnees-personnelles.php

- http://www.latribune.fr/opinions/tribunes/20140618trib000835759/objets-connectes-attention-a-l-espionnage-domestique.html

Copyright © 2024 Légavox.fr - Tous droits réservés