Données personnelles
La sécurité des données à l'ère des objets connectés

Thermostats, serrures, réfrigérateurs, télévisions : nos foyers seront bientôt entièrement équipés d'objets capables de voir, d'entendre, d'analyser la température ou la luminosité de nos intérieurs. L'impact économique considérable de ces technologies sera toutefois lié au traitement de masse de nos données personnelles, ce qui pose de nouvelles interrogations en matière de sécurité.

La révolution de « l'Internet des objets » est en marche. Selon l'IDATE, l'Institut de l'audiovisuel et des télécommunications en Europe, 15 milliards d'objets sont aujourd'hui connectés dans le monde, et devraient atteindre le nombre impressionnant de 80 milliards en 2020 (1). A l'ère de la connexion permanente, et dans un but de faciliter notre quotidien, ces objets transmettent nécessairement à leurs concepteurs des informations sur nos modes de vie, nos centres d'intérêts, et même notre santé. Les risques liés à leur utilisation et l'encadrement par la seule loi Informatique et libertés posent donc de nouveaux défis pour la sécurité et la protection des données personnelles.

LES RISQUES LIES À L'UTILISATION DES OBJETS CONNECTES

Le traitement massif des données obtenues par les objets connectés s'inscrit dans le phénomène du Big Data, qui soulève de nombreuses inquiétudes en matière de sécurité. Dès lors, ces ensembles de données, notamment sensibles car souvent relatives à la santé ou au bien-être de l'utilisateur, courent le risque potentiel d'être rendues accessibles à des tiers mal intentionnés ou de porter atteinte à la vie privée des personnes concernées.

Les objets connectés : futur du Big Data

Selon le cabinet de conseil McKinsey, les objets connectés devraient représenter d'ici 2025 entre 2700 et 6200 milliards de dollars de valeur ajoutée pour l'économie mondiale (2). A la lecture de ces chiffres, on comprend aisément que l'exploitation des données personnelles des consommateurs est le fondement de l'économie des objets connectés. Généralement jumelés à un smartphone, sur lequel est installée une application dédiée, ou plus simplement connectés à un réseau sans fil, les objets connectés rendent aux utilisateurs des services de toutes sortes et possèdent des capteurs leur permettant de collecter et de traiter des informations. Le fabricant français Parrot a par exemple développé un concept de sonde à planter dans le bac d'une plante pour surveiller l'hydrométrie, la luminosité et la fertilité du sol, des notifications étant adressées sur le smartphone de l'utilisateur lorsque la plante a besoin d'eau ou d'engrais. La société Nest Labs, rachetée en début d'année par Google pour 2,3 milliards d'euros, propose quant à elle le thermostat intelligent Nest qui enregistre les habitudes des utilisateurs et programme à distance la température de la maison.

Ces données sont nécessairement variées, générées dans des temps très courts, et transmises en très grandes quantités. Elles s'inscrivent donc dans le Big Data, qui fait référence aux ensembles volumineux de données et aux outils nécessaires pour les traiter et les analyser rapidement. Or le Big Data inquiète. Si les traitements de données à caractère personnel sont régis en France par les dispositions de la loi « Informatique et libertés » du 6 janvier 1978, et celles de la Directive 95/46/CE du 24 octobre 1995, les questions relatives à la finalité des traitements, à leur proportionnalité et à leur pertinence risquent d'être laissées de côté par les concepteurs d'objets connectés. En effet, il n'est pas certain que les fabricants intègrent dès la conception de l'objet les dispositifs techniques nécessaires au respect de la législation, ce qui serait pourtant un gage de sécurité pour les consommateurs.

Par ailleurs, les informations variées produites et partagées par les utilisateurs peuvent notamment servir à alimenter des bases de données à des fins de profilage, de ciblage publicitaire ou de communication, d'où leur grande valeur. Couplées à des bases de données provenant des réseaux sociaux, des sites de streaming ou de e-commerce, les informations collectées par les objets connectés participent grandement à la « datafication », ce phénomène consistant à convertir nos interactions avec ce qui

nous entoure en données exploitables. Or les informations sur le stockage des données personnelles ne sont pas toujours communiquées de manière transparente, et la question de l'obtention du consentement du consommateur dans le traitement de ses données personnelles prend ici tout son sens.

Santé connectée et « quantified self »

Les objets connectés ne se limitent pas à l'invasion des foyers. De nouvelles pratiques d'auto-mesure du corps, destinées à améliorer nos habitudes de vie, sont apparues. Le « quantified self », ou quantification du soi, est un phénomène alimenté par l'apparition de montres, bracelets et autres objets connectés mesurant le sommeil, le rythme cardiaque, le nombre de calories brûlées lors d'une activité sportive, etc. Comme pour la domotique, ces données relatives au bien-être de l'individu sont acheminées vers les serveurs du fabricant, qui les analyse et les retransmet au consommateur.

Or la frontière entre les données relatives au bien-être et les données de santé est encore floue. La donnée de santé n'est définie par aucun texte, mais l'on s'accorde à dire qu'il s'agit d'une donnée susceptible de révéler l'état pathologique de la personne qu'elle concerne. L'article 4 du projet de règlement européen sur la protection des données personnelles propose toutefois de définir la donnée de santé comme « *toute information relative à la santé physique ou mentale d'une personne, ou à la prestation de services de santé à cette personne* » (3).

La donnée de santé fait ainsi l'objet d'un encadrement particulier. Concernant l'hébergement de données de santé, l'article L.1111-8 du Code de la santé publique issu de la loi n° 2002-303 du 4 mars 2002 relative aux droits des patients impose à l'hébergeur de données de santé d'obtenir un agrément préalable du ministre chargé de la santé. Enfin, les données de santé sont considérées par la loi Informatique et libertés comme des données sensibles dont le traitement et la collecte sont par principe interdits, à moins que la personne concernée n'ait donné son consentement exprès.

Ainsi, l'enjeu principal tient à la qualification des données collectées par les objets connectés, lesquelles, sous couvert d'améliorer le bien-être des utilisateurs, peuvent facilement s'apparenter à des données relatives à leur santé. Et comme l'utilisation gratuite d'un service se fait rarement sans contrepartie, les inquiétudes quant à la finalité des traitements de telles données s'avèrent fondées. A ce titre, la Cnil a recommandé au public d'utiliser, si possible, un pseudonyme pour partager les données, de ne pas automatiser le partage des données vers d'autres services (notamment vers les réseaux sociaux), de ne publier les données qu'en direction de cercles de confiance et d'effacer ou de récupérer les données lorsqu'un service n'est plus utilisé (4).

Piratage, usurpation d'identité, vie privée, réputation

La sécurité des traitements de données obtenues au moyen d'objets connectés devient un véritable enjeu. Avec l'Internet des objets, il existe un risque non négligeable que les pirates s'invitent dans les maisons, en détournant les informations relatives aux allées et venues des propriétaires, enregistrées par les serrures connectées ou synchronisées par des applications smartphones dédiées. Il n'est pas non plus insensé d'imaginer des hackers intégrer des virus aux objets connectés ou pénétrer frauduleusement dans des data centers et s'approprier la vie numérique et l'identité d'un individu. Des experts en sécurité informatique ont également démontré comment désactiver à distance les freins d'une voiture électrique ou prendre le contrôle d'un pacemaker avec un simple ordinateur.

Les problématiques de confidentialité intéressent également le droit au respect de la vie privée, bien que l'achat d'un objet qui révèle nos habitudes semble présenter une certaine incompatibilité avec la volonté de protéger son intimité. Les exigences de confidentialité ont notamment pris une nouvelle dimension avec l'apparition d'objets tels que la « Google glass », cette paire de lunettes connectés qui permet notamment à ses utilisateurs de photographier, filmer ou « tagguer » sur des réseaux sociaux leurs interlocuteurs à leur insu, au risque de porter atteinte à leur image ou leur réputation. Le problème du consentement de ces derniers n'est d'ailleurs pas résolu. Or l'article 226-22 du code pénal punit de cinq ans d'emprisonnement et de 300 000 euros d'amende le fait, pour une personne qui a recueilli des données à caractère personnel « *dont la divulgation aurait pour effet de porter atteinte à la considération de l'intéressé ou à l'intimité de sa vie privée, de porter, sans autorisation de l'intéressé, ces données à la connaissance d'un tiers qui n'a pas qualité pour les recevoir* ».

Par ailleurs, les technologies permettant la géolocalisation, si elles offrent aux individus une avancée certaine en matière de services, posent toutefois la question de la traçabilité des personnes. Les montres et voitures connectées qui proposent généralement des cartes et itinéraires, localisent nécessairement leur propriétaire. La crainte d'une surveillance généralisée n'a d'ailleurs pas été balayée par la loi n° 2014-372 du 28 mars 2014 relative à la géolocalisation, qui a au contraire créé l'article 230-32 du code de procédure pénale, au terme duquel les enquêteurs peuvent recourir dans certains cas « *à tout moyen technique destiné à la localisation en temps réel, sur l'ensemble du territoire national, d'une personne, à l'insu de celle-ci, d'un véhicule ou de tout autre objet, sans le consentement de son propriétaire ou de son possesseur* ». La possibilité qu'un individu puisse être localisé grâce à sa brosse à dents connectée se dessine…

UN DISPOSITIF LEGISLATIF MODESTE A L'HEURE DES MONTRES CONNECTEES

Face aux risques liés à la démocratisation prochaine des objets connectés, l'encadrement juridique de ces

technologies pourrait aujourd'hui se montrer insuffisant, alors qu'un « droit à la désactivation » des objets connectés semble d'ores et déjà réclamé par les consommateurs. Une réflexion sur l'adaptation ou la création des règles applicables à l'Internet des objets s'avère donc nécessaire.

Un encadrement juridique déconnecté ?

De manière générale, la loi Informatique et libertés oblige l'organisme responsable du traitement des données à en préserver la sécurité. D'après les dispositions de l'article 34, « *le responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès* ». L'article 226-17 du code pénal punit ainsi de cinq ans d'emprisonnement et de 300 000 euros d'amende le non-respect de ces dispositions. Pour les personnes morales, l'amende peut être multipliée par 5 et atteindre jusqu'à 1.500.000 euros (5).

En outre, les atteintes aux systèmes de traitement automatisé de données, en cas d'accès ou de maintien frauduleux, sont punies de deux ans d'emprisonnement et de 30.000 euros d'amende, en vertu des dispositions de l'article 323-1 du code pénal, issu de la loi n°88-19 du 5 janvier 1988 dite « Godfrain ». Si des données ont été introduites, modifiées ou supprimées, les sanctions passent à cinq ans d'emprisonnement et 75.000 euros d'amende (6).

Or des interrogations subsistent quant au caractère dissuasif de ces sanctions, au regard du volume de données personnelles concernées et des conséquences d'un piratage de celles-ci. Une réévaluation des peines prévues par le code pénal et la condamnation à des amendes plus importantes pourrait décourager certains délinquants. De même, si en France, les traitements de données personnelles sont a minima soumis à une déclaration auprès de la Cnil, on peut imaginer que l'ensemble des fabricants ou des distributeurs d'objets connectés, en tant que responsables de traitements, ne respecteront pas les obligations de déclaration ou n'attendront pas l'autorisation de la Cnil pour commercialiser leurs nouveautés. Il convient toutefois de noter que le futur règlement européen comporte de nouvelles mesures relatives aux sanctions, dont le montant maximal pourrait varier en fonction du chiffre d'affaires global de l'entreprise en cause.

Enfin, les sanctions encourues en cas de non respect des règles en matière de transfert de données personnelles hors Union Européenne, à savoir 300 000 euros d'amende et 5 ans d'emprisonnement, peuvent également sembler dérisoires. Concernant les Etats-Unis, qui ne disposent pas d'un niveau adéquat de protection des données, les responsables américains de traitements de données provenant d'objets connectés devront adhérer aux principes du Safe Harbor pour pouvoir effectuer des transferts de données vers leur pays. Ce mécanisme basé sur l'auto-adhésion prête toutefois à sourire, quand on sait que Facebook y a adhéré. D'autant que le Patriot Act du 26 octobre 2001 permet aux agences américaines de renseignement d'accéder à toute donnée personnelle hébergée par un prestataire américain en cas de suspicion de terrorisme ou d'espionnage. En tout état de cause, si les objets connectés constituent une mine d'informations titanesque, il n'est pas sûr que l'encadrement juridique actuel leur soit véritablement adapté.

Responsabilité et reconnaissance d'un « droit à la désactivation »

Les objets connectés pourront remplacer l'individu dans certaines de leurs habitudes, et notamment d'achat. Les réfrigérateurs seront par exemple bientôt connectés, et les distributeurs ont déjà imaginé des partenariats avec les fabricants pour passer automatiquement commande lors de l'épuisement des produits. Or l'objet connecté ne bénéficie encore d'aucun statut juridique, ce qui peut générer des difficultés lors de la conclusion de contrats, de la transmission du consentement du consommateur, et même du paiement. Les risques d'erreur ou de défaillance de l'objet connecté alimenteront nécessairement les conditions générales d'utilisation en clauses limitatives de responsabilité de la part des fabricants. Les problématiques de responsabilité du fait des choses, bien qu'intelligentes, connaîtront également un nouvel essor, notamment en cas d'accident de la circulation impliquant un véhicule à conduite automatisée de type Google Car. Reste à espérer que les assureurs ne limiteront pas la prise en charge des dommages causés par des objets connectés, à moins qu'une assurance spéciale ne voie le jour…

Le développement des objets connectés est d'ailleurs une grande opportunité pour les assureurs, dans un contexte particulièrement concurrentiel. En matière de bien-être et de santé, et dans une logique de réduction des risques, certaines compagnies d'assurances analysent déjà les habitudes de conduite de leurs assurés ou leur dernière prise de tension par un bracelet connecté, et les alertent sur les risques médicaux encourus. Des offres tarifaires particulières pourraient alors être réservées aux assurés qui prennent soin de leur santé. Les services d'assistance pourront être améliorés par les objets contenant des fonctionnalités de géolocalisation.

Face aux risques que comportent ces nouvelles utilisations, une hypothèse particulière doit être envisagée, celle d'un consommateur décidant finalement de désactiver la connexion de l'appareil et le partage des données. Si l'objet connecté risque de perdre beaucoup de son intérêt, le fabricant ne pouvant plus analyser les informations et fournir le service initial, certains objets resteront sans nul doute utiles à leurs utilisateurs, même de manière traditionnelle, telle qu'un pèse-personne connecté. Certains avancent donc déjà un droit à la désactivation ou « au silence » des puces, permettant aux individus concernés de retirer leur consentement, de manière immédiate et même physique, en débran-

chant l'appareil ou en appuyant sur un bouton. A cette fin, l'intégration de cette fonctionnalité devrait être prévue dès la conception de l'objet.

Une réflexion prospective nécessaire

Au vu des risques potentiels et du cadre juridique actuel, une réflexion des acteurs des technologies connectées s'impose pour accompagner et sécuriser leur développement. Une première piste consisterait à faire entendre aux industriels l'intérêt d'intégrer des systèmes de protection de la vie privée dès la conception des objets, illustré par le concept de « privacy by design » que le Parlement européen souhaite d'ailleurs imposer aux responsables de traitements (7). Des procédures de labellisation ou de certification pourraient également être prévues pour mettre en lumière les entreprises soucieuses du respect de la réglementation des données personnelles. La Cnil pourrait à ce titre se voir confier la responsabilité d'auditer et de récompenser ces responsables de traitement, étant entendu que la protection des données personnelles s'avèrera bientôt un argument économique puissant pour les consommateurs.

De surcroît, la sensibilisation des utilisateurs s'avère indispensable. De manière générale, il est recommandé de mettre à jour et dès sa sortie tout objet connecté avec les correctifs de sécurité du constructeur. L'accès des objets vers le monde extérieur, par le biais d'Internet notamment, doit être également surveillé. L'installation de pare-feu et d'antivirus sur les ordinateurs est une première barrière de sécurité. Dans les entreprises, les responsables de la sécurité des systèmes d'information (RSSI) doivent également prendre en compte les fonctionnalités de communication de ces objets pour assurer la fiabilité des usages. Les règles applicables en matière de géolocalisation des salariés doivent notamment être respectées, au regard du développement des voitures connectées. Un arrêt de la Cour de cassation en date du 3 novembre 2011 a en effet déclaré illicite la surveillance par géolocalisation des salariés sans les avoir préalablement informés (8).

Certaines autorités indépendantes et autres commissions se penchent à l'heure actuelle sur la définition d'un encadrement adapté pour les objets connectés. Le Commissariat général à la stratégie et à la prospective (CGSP) a engagé mi-avril une réflexion sur l'Internet des objets en vue de formuler des recommandations à l'égard de la puissance publique, afin de l'aider à répondre aux défis futurs d'internet (9). Le Conseil National du Numérique a également lancé une concertation sur la santé et le numérique, avec pour objectif une réflexion sur les perspectives actuelles liées à la e-santé, dont font partie les objets connectés (10). Pour sa part, la Cnil a lancé l'an dernier un chantier de réflexion au sujet de la santé et du bien-être dans le monde numérique.

Enfin, en matière de santé des utilisateurs, il convient de noter que les députés ont adopté le 23 janvier dernier une proposition de loi « *relative à la sobriété, à la transparence et à la concertation en matière d'exposition aux ondes électromagnétiques* », visant à une meilleure information et sensibilisation du public sur les sources d'émission des appareils radioélectriques. Les objets connectés, dont certains comportent des puces RFID leur permettant de communiquer avec l'environnement, sont donc concernés par ces dispositions.

CONCLUSION

Entre simples moyens de communication ou véritables acteurs juridiques, il convient désormais de donner une qualification aux objets connectés et de clarifier le régime juridique qui leur est applicable. Le défi est à la fois juridique et éthique, avec pour objectif premier de rassurer le consommateur face au volume massif de données personnelles qui est traité. Le risque de piratage de données, qu'elles soient sensibles ou encore révélatrices de notre vie privée, pourrait en effet limiter le potentiel économique phénoménal de l'Internet des objets. Si les individus restent libres de ne pas utiliser d'objets connectés, il serait préférable de trouver un juste équilibre entre sécurité des données et avancées technologiques.

Caroline LAVERDET
Avocat à la cour

(1) IDATE, « The Internet of Things », rapport publié le 26 août 2013
(2) McKinsey Global Institute, « Disruptive technologies: Advances that will transform life, business, and the global economy », rapport publié en mai 2013, p. 12
(3) Proposition de règlement du Parlement Européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données en date du 25 janvier 2012
(4) Quantified Self : comment mieux se connaitre grâce à ses données, 26 nov. 2012, Cnil
(5) Article 131-18 du code pénal
(6) Article 323-3 alinéa 1 du code pénal
(7) Article 23 de la proposition de règlement en date du 25 janvier 2012, voir note préc. n°3
(8) Cour de cassation, Soc., 3 novembre 2011, pourvoi n° 10-18.036, Moreau incendies / M. Eric X.
(9) Communiqué – L'internet des objets, 14 avril 2014, http://www.strategie.gouv.fr
(10) http://www.cnnumerique.fr/sante