Objets connectés, vie privée et données personnelles : une équation difficile pour protéger l'utilisateur

Malgré un vaste arsenal juridique limitant les impacts négatifs des objets connectés, les risques d'intrusions demeurent pour les utilisateurs de ces appareils – du compteur électrique à la montre connectée, en passant par la « mesure de soi ». Recueillir leur consentement est un préalable.

Par Christiane Féral-Schuhl*, avocate associée, cabinet Féral-Schuhl/Sainte-Marie

Selon une étude menée par Gartner, 20 milliards d'objets connectés seraient en circulation en 2020 (1). Qu'il s'agisse du domaine de la santé, du bien-être, du sport, de la domotique ou encore du loisir, l'attrait des utilisateurs pour les objets connectés est caractérisé. Paradoxalement, bien qu'avertis, ces derniers ne mesurent pas toujours les risques qui pèsent sur leur vie privée et leurs données personnelles. Ces deux notions – vie privée et données personnelles – ne sont pas synonymes, bien qu'intrinsèquement liées (2).

Les exemples de Linky et de Gazpar

La donnée personnelle se définit comme *« toute information se rapportant à une personne physique identifiée ou identifiable »* (3). A l'inverse, la vie privée ne trouve pas de définition légale bien que le Code civil consacre un droit au respect de la vie privée (4). Les apports de la jurisprudence permettent aujourd'hui de définir la notion de vie privée comme *« le droit pour une personne d'être libre de mener sa propre existence avec le minimum d'ingérences extérieures »* (5). Ainsi, si un objet connecté peut porter atteinte aux données personnelles d'un utilisateur (collecte illicite des données personnelles, failles de sécurité permettant aux tiers d'accéder aux données, etc.), il peut également dans une plus large mesure porter atteinte à sa vie privée (captation d'images ou de voix, intrusion dans l'intimité, etc.). L'ubiquité et l'omniprésence des objets connectés dans la vie des utilisateurs conduisent à une collecte permanente et instantanée des données. Par ce biais, de nombreuses informations relatives à la vie privée des utilisateurs deviennent identifiables. D'ailleurs, la divulgation massive de données relatives à la vie privée lors de l'utilisation d'un objet connecté est souvent une condition *sine qua non* à l'existence du service proposé par le fabricant. A titre d'exemple, la nouvelle génération de compteurs d'électricité et de gaz, tels que respectivement Linky et Gazpar qui ont fait l'objet d'une communication (6) de la Cnil en novembre 2017, peut collecter des données de consommation énergétique journalières d'un foyer. Si l'utilisateur y consent, des données de consommation plus fines peuvent être collectées par tranche horaire et/ou à la demi-heure. Cela permet d'avoir des informations très précises sur la consommation énergétique de l'usager. Dans l'hypothèse d'un traitement insuffisamment sécurisé, une personne malveillante pourrait alors avoir accès à des informations telles que les plages horaires durant lesquelles l'usager est absent de son logement, celles pendant lesquelles il dort ou encore les types d'appareils utilisés. Les habitudes d'une personne peuvent ainsi être déterminées aisément, ce qui constitue une atteinte à la vie privée. La décision de la Cnil, datée du 20 novembre 2017 et mettant demeure la société Genesis Industries Limited (7), est une autre illustration des risques encourus par l'utilisation des objets connectés notamment au regard de la vie privée. Cette société commercialisait des jouets connectés qui pouvaient interagir avec les enfants. Suite à un contrôle effectué par la Cnil, il a été constaté une absence de sécurisation des jouets (8) qui permettait à toute personne possédant un dispositif équipé d'un système de communication Bluetooth de s'y connecter à l'insu des personnes et d'avoir accès aux discussions échangées dans un cercle familial ou amical (9). L'intrusion dans la vie privée à travers les objets connectés peut ainsi être importante et particulièrement dangereuse lorsqu'il s'agit d'un utilisateur vulnérable tel qu'un enfant mineur.

Pour autant, une réglementation est difficilement applicable aux objets connectés. Tout d'abord, une incompatibilité d'origine des objets connectés avec certains principes relatifs au traitement des données personnelles doit être soulignée.

Proportionnalité, mesure de soi et Big Data

A titre d'exemple, le principe de proportionnalité (10), qui requiert que les données soient adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées, ne peut être satisfait dans le cadre de l'utilisation d'un objet connecté dit *quantified-self* – c'est-à-dire un appareil connecté pour la « mesure de soi ». En effet, le nombre de données collectées sera nécessairement important pour qu'un service adapté à l'utilisateur puisse être fourni. De même le principe de conservation limité des données collectées (11) peut difficilement être mis en application dans le cadre d'un service fourni par un objet connecté. En effet, la conservation des données pour une durée indéterminée représente souvent une opportunité pour les fabricants dans le cadre du Big Data.

Notes

(1) - Connected "Things" 07-02-17 : https://lc.cx/MTBg

(2) - Loi n° 78-17 du 6 janvier, article 1.

(3) - Article 4 du règlement européen 2016/679.

(4) - Article 9 du Code civil. Les articles 226-1 et suivants du Code pénal incriminent également les atteintes à la vie privée.

(5) - Voir l'arrêt de la Cour européenne des droits de l'homme (CEDH) du 29 avril 2002, Pretty c/ Royaume-Uni.

(6) - Communication de la Cnil du 21-11-17 : https://lc.cx/MTa6. Voir aussi les recommandations de la Cnil datées du 15-11-12 : https://lc.cx/MTRj

(7) - Sur le fondement de l'article 1er de la loi du 6 janvier 1978 modifiée.

Aujourd'hui, en vertu de la loi « Informatique et Libertés », une obligation d'information pèse sur les responsables de traitement (12). De même, en vertu du Code de la consommation, une obligation précontractuelle d'information pèse sur le professionnel qui propose un bien ou un service (13). L'utilisateur d'un objet connecté doit ainsi pouvoir avoir des informations claires et précises sur le traitement de ses données, mais également sur les caractéristiques de l'objet connecté.

Loi française et règlement européen

Or, la récente assignation de deux plateformes majeures dans le monde numérique – notamment sur le fondement de pratiques commerciales trompeuses au motif d'un non-respect de l'obligation précontractuelle d'information dans le cadre de la vente d'objets connectés (14) – souligne les difficultés relatives à l'information des utilisateurs. L'avis de 2014 du G29, le groupe qui réunit les « Cnil » européennes, sur les objets connectés illustre également le manque d'informations des utilisateurs sur le traitement de leurs données (15). Ainsi, bien qu'une réglementation protectrice des utilisateurs d'objets connectés soit applicable, celle-ci est difficilement mise en œuvre. De cet obstacle découle la question de la validité du consentement de l'utilisateur. Si le droit à l'autodétermination informationnelle – droit pour toute personne de décider et de contrôler les usages qui sont faits des données à caractère personnel la concernant, dans les conditions fixées par la loi « Informatique et libertés » – a été récemment affirmé en France, son effectivité au regard des objets connectés semble moindre. En effet, même si au moment de l'activation de l'appareil le consentement à la collecte de certaines données est recueilli auprès de l'utilisateur, il convient de souligner que par la suite des données sont délivrées de manière involontaire. Par exemple, dans le cadre d'une montre connectée, l'utilisateur consent à la collecte de données relatives au nombre de pas qu'il effectue au cours de la journée. Mais lors de cette collecte, le responsable de traitement peut également avoir accès à d'autres données telles que celles relatives à la géolocalisation de l'utilisateur. En ce sens, le consentement recueilli n'est pas toujours éclairé et le droit à l'autodétermination informationnelle n'en sera qu'affaibli. Ainsi, la protection de l'utilisateur d'un objet connecté semble moindre. L'applicabilité du règlement européen sur la protection des données personnelles le 25 mai prochain – règlement dit RGPD pour « règlement général sur la protection des données » (16) – permet d'envisager une amélioration de la protection des utilisateurs d'objets connectés sur plusieurs points. Tout d'abord, par l'exigence de la mise en place de mesures permettant d'assurer une protection de la vie privée par défaut et dès la conception de l'objet connecté, le fabricant sera amené à prendre en compte les questions relatives à la vie privée de l'utilisateur en amont d'un projet (17). De même, les nouvelles mesures de sécurité devant être prises, tant par les responsables de traitement que les sous-traitants (par exemple, la pseudonymisation, les tests d'intrusion réguliers, ou encore le recours à la certification), tendront à garantir une meilleure protection des données personnelles des utilisateurs (18). Ensuite, la mise en place de nouveaux droits pour l'utilisateur tels que le droit d'opposition à une mesure de profilage (19), le droit d'effacement des données pour des motifs limitativement énumérés (20) ou encore le droit à la portabilité des données (disposition déjà introduite par la loi « République numérique » du 7 octobre 2016 dans le Code de la consommation aux articles L. 224-42-1 et suivants) consolideront les moyens conférés aux utilisateurs d'objets connectés pour protéger leur vie privée. Il convient de souligner que cette amélioration dépend tout de même d'une information effective de l'utilisateur. En effet, si le fabricant ou le distributeur de l'objet n'informe pas l'utilisateur des différents droits dont il dispose, il semble peu probable que les utilisateurs les moins avertis agissent. Enfin, si la question de l'applicabilité de la réglementation européenne pour les acteurs situés en dehors de l'Union européenne (UE) pouvait se poser notamment lorsqu'ils collectaient des données d'utilisateurs européens, celle-ci n'aura plus lieu d'être à compter du 25 mai 2018. En effet, tout responsable de traitement ou sous-traitant qui n'est pas établi dans l'UE dès lors qu'il collectera des données personnelles de personnes se trouvant sur le territoire de l'UE sera contraint de respecter la réglementation européenne relative aux données personnelles. Ce point est important puisque dans le cadre des objets connectés, souvent, les flux de données ne connaissent pas de frontières.

Gagner la confiance du public

L'équation objets connectés, vie privée et données personnelles est par définition difficile. La révélation massive et constante de données relatives à une personne implique nécessairement une intrusion importante et parfois non voulue dans la vie des utilisateurs. Cependant, l'existence d'un arsenal juridique tant en droit français qu'en droit européen permet de limiter les impacts négatifs générés par les objets connectés. D'ailleurs il convient de noter que, dans le récent cadre de la réécriture de la loi « Informatique et Libertés », la commission des lois a adopté un amendement permettant à une personne concernée d'obtenir réparation au moyen d'une action de groupe du dommage causé par un manquement du responsable de traitement ou sous-traitant aux dispositions de cette loi. Finalement, dans un marché hautement concurrentiel, les objets connectés qui survivront seront ceux qui auront su gagner la confiance du public et présenteront le plus de garanties en matière de respect à la vie privée et de sécurité. @

** Ancien bâtonnier du Barreau de Paris, et auteure de « Cyberdroit », dont la 7e édition (2018-2019) paraîtra en novembre 2017 aux éditions Dalloz.*

Notes

(8) - En l'occurrence la poupée « My Friend Cayla » et le robot « I-Que ».

(9) - Décision « Genesis Industries Limited » du 20-11-17 : https://lc.cx/MTHT

(10) - Il y a d'autres principes tels que le principe de conservation des données pendant une durée limitée ou encore le principe de minimisation des données.

(11) - Article 6, 3° et 5° de la loi « Informatique et libertés ».

(12) - Article 32 de la loi « Informatique et libertés ».

(13) - Code de la consommation, Article L111-1.

(14) - Assignation de la Fnac et Amazon devant le TGI de Paris, par UFC-Que Choisir le 09-01-18 : https://lc.cx/MTFN

(15) - « Avis 8/2014 sur les récentes évolutions relatives à l'internet des objets », adopté par le « G29 » le 16-09-14 : https://lc.cx/MTtu

(16) - Règlement 2016/679 dit RGPD du 27 avril 2016 : https://lc.cx/DP-16.

(17) - Article 25 (RGPD).

(18) - Article 25 (RGPD).

(19) - Article 25 (RGPD).

(20) - Article 25 (RGPD).