

Données personnelles et objets connectés : quels défis ?

Les choix qui s'offrent aux consommateurs concernant le partage et le traitement de leurs informations personnelles avec l'Internet des objets doivent être clarifiés. Une réflexion s'impose pour conserver la maîtrise de ces données. L'enjeu a une dimension collective.

Pascal Pichonnaz

Abrégé Le règlement européen et la loi fédérale sur la protection des données posent l'exigence du consentement pour le partage de données. Or, les consommateurs ne pourront jouer leur rôle sur le marché que si les producteurs d'objets interconnectés leur donnent un véritable choix, tant sur la participation aux bénéfices économiques des données collectées que sur la transmission de ces informations à des tiers désignés. Une prise de conscience est nécessaire : une vraie maîtrise des données par les consommateurs implique de tenir compte de la dimension collective des données à caractère personnel. Une gestion des différends par des actions judiciaires collectives devrait aussi favoriser ce but.

Dans la société numérisée, chaque consommateur produit de très nombreuses données. Celles-ci sont souvent récoltées, agrégées et réutilisées pour rendre toutes sortes de services. C'est déjà le cas aujourd'hui, non seulement lors de l'usage de nos smartphones et de nombreuses applications, mais aussi pour divers véhicules automobiles qui envoient des informations en continu aux constructeurs. Dès lors, les consommateurs peuvent-ils encore avoir la maîtrise de toutes les données qu'ils produisent quotidiennement ? C'est toute la question de la « maîtrise des données » (ou « Datenhoheit »).

Le règlement de l'Union européenne sur la protection des données (RGPD)² vise à protéger les personnes physiques lors du traitement de données à caractère personnel. Il exige que le traitement de ce type d'informations soit consenti pour une ou plusieurs finalités spécifiques, sauf si des intérêts supérieurs et légitimes (d'ordre privé ou public) permettent de s'en passer.

Le champ d'application du RGPD européen ne se recoupe pas totalement avec l'actuelle loi fédérale sur la protection des données (LPD), puisque cette dernière protège non seulement les personnes physiques, mais aussi les personnes morales. Pour que le traitement soit licite, la LPD exige en revanche également le consentement de la victime

ou des intérêts prépondérants de la personne qui traite des données personnelles. Néanmoins, « en règle générale, il n'y a pas atteinte à la personnalité lorsque la personne concernée a rendu les données accessibles à tout un chacun et ne s'est pas opposée formellement au traitement »³. Le RGPD est notoirement plus restrictif, ce qui a justifié la mise en œuvre d'une réforme de la LPD en 2017⁴. On peut néanmoins affirmer que la personne physique est bien protégée dans la LPD : dès qu'elle fait l'objet d'un traitement de « données à caractère personnel », elle doit soit donner son consentement, soit avoir eu un comportement qui laisse présumer un tel consentement (avant tout rendre les données accessibles à chacun) pour que le traitement soit licite.

L'enjeu des données anonymisées

La LPD définit les données personnelles comme étant « toutes les informations qui se rapportent à une personne identifiée ou identifiable »⁵. Le RGPD adopte une approche similaire considérant que les « données à caractère personnel » comprennent « toute information se rapportant à une personne physique » qui « peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de

localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale »⁶. Partant, un processus d'anonymisation de la récolte de données pourrait permettre d'échapper au RGPD ; toutefois, c'est justement certaines caractéristiques personnelles qui intéressent l'exploitation des données (ou « data mining » en anglais) et le traitement de données à caractère personnel. L'anonymisation complète est dès lors souvent incompatible avec le but recherché.

Avec l'entrée en vigueur du RGPD, des fenêtres se sont ouvertes sur nos smartphones, ordinateurs et tablettes pour nous permettre de consentir au traitement de toutes sortes de données à caractère personnel. Le consentement constitue ainsi l'une des sources de protection. Il est d'ailleurs possible – du moins en théorie – de retirer à tout moment son consentement⁷. Le RGPD protège également les personnes physiques en imposant des exigences de protection pour les données récoltées⁸ : ces devoirs nécessitent des mesures techniques et organisationnelles appropriées (« privacy by design » ou « respect de la vie privée dès la conception » en français). Le RGPD impose par défaut un traitement limité aux données nécessaires au vu de la finalité spécifique. Une fois adaptée au niveau de protection européen, la LPD confèrera elle aussi une maîtrise de ses données à tout un chacun.

Un colosse aux pieds d'argile

La multiplication des consentements donnés par les consommateurs, via la conclusion de contrats ou par le biais d'un consentement spécifique, a créé une situation préoccupante. En effet, personne n'est en mesure de

¹ Voir notamment CFC (2017).

² Journal officiel de l'Union européenne, L 119, 4 mai 2016, p. 1.

³ Art. 12 al. 3 LPD.

⁴ Conseil fédéral (2017).

⁵ Art. 3 let. a LPD.

⁶ Art. 4 ch. 1 RGPD.

⁷ En vertu de l'art. 7 al. 3 RGPD.

⁸ Art. 25 RGPD.

déterminer aujourd'hui à quelles fins il a déjà donné son consentement pour l'usage de données à caractère personnel.

Cette situation produit deux phénomènes : d'une part, le sentiment d'avoir largement consenti à l'usage de données à caractère personnel tend à banaliser l'octroi du consentement, voire amène à le considérer comme une chicane inutile par nombre d'utilisateurs ; d'autre part, la tentation est grande de se préoccuper avant tout des données personnelles sensibles, pour lesquelles un consentement exprès et des devoirs d'annonce spécifiques sont requis. Le résultat est ainsi d'affaiblir largement la protection envisagée pour les données à caractère personnel « ordinaire ».

Prenons l'exemple des objets interconnectés. À l'horizon 2025, pas moins de 22 milliards de ces objets devraient être utilisés à travers le monde⁹. Pour les consommateurs, l'Internet des objets (IdO)

représente de nouvelles fonctionnalités et de nouveaux modes d'agir au quotidien qui devraient faciliter la vie de chacun. Fantastique opportunité de personnaliser les biens et les services de toutes sortes (consommation courante, énergie, santé, etc.), l'IdO représente toutefois aussi des défis pour le consommateur et ses droits.

La mise en réseau de l'IdO présente d'abord des risques pour les entreprises, notamment celui d'ouvrir des brèches dans la sécurité informatique, qui peuvent permettre à des pirates d'atteindre des données essentielles de l'entreprise, mais aussi bien sûr des données personnelles de consommateurs. Pour ces derniers, le traitement de données (« data management » en anglais) doit être consenti et surtout connu. C'est là un enjeu difficile. Pour augmenter la confiance dans les objets interconnectés, les consommateurs doivent être suffisamment informés du fonctionnement du traitement des données. Il faut dès lors assurer un régime d'information et de protection adéquat du consommateur ; or, cette information devrait aussi passer par des choix.

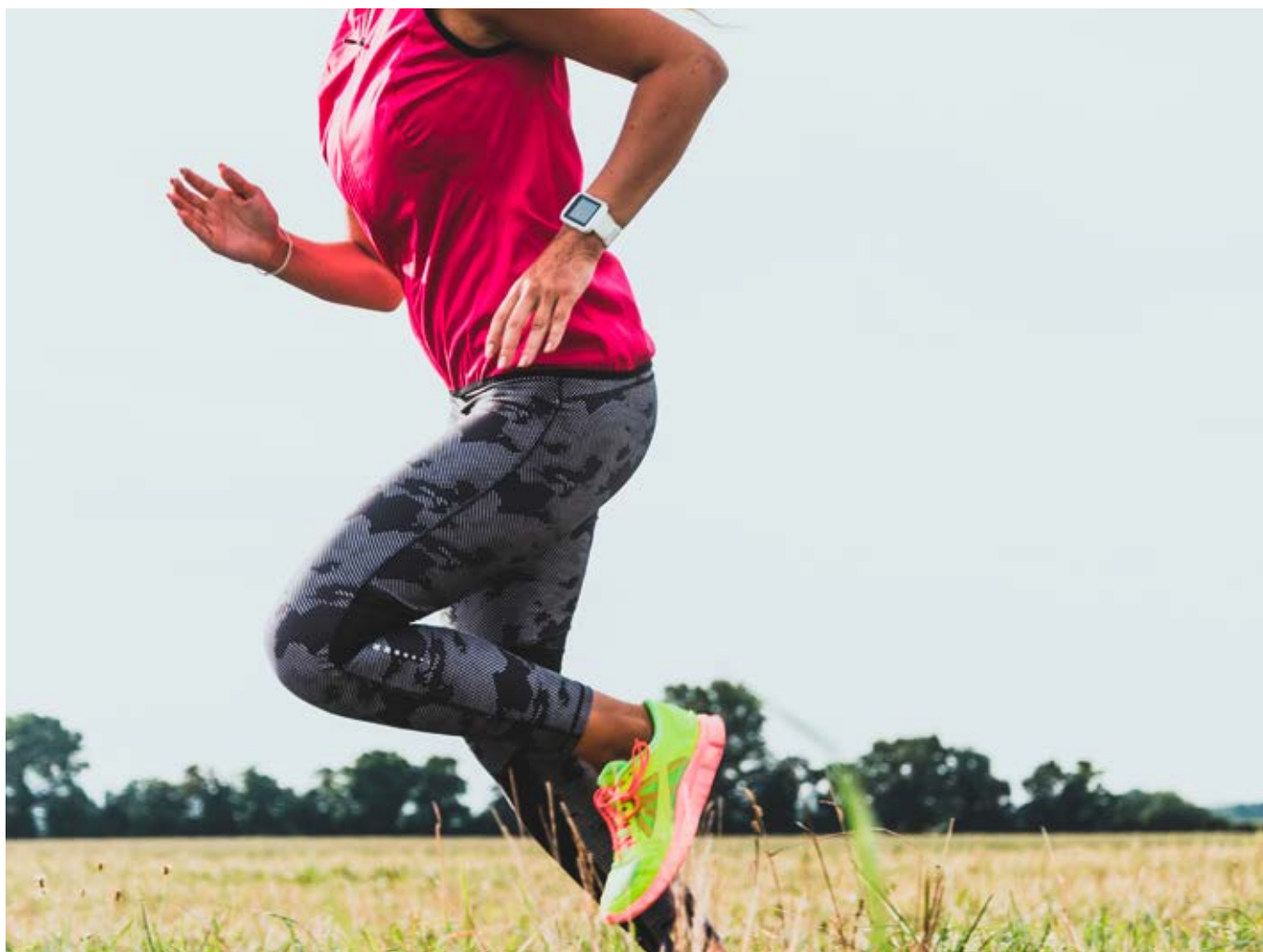
L'importance d'un choix plus ouvert

Les données personnelles présentent certes un intérêt pour les entreprises technologiques – et autres – désireuses d'améliorer la fiabilité et la sécurité des produits interconnectés qu'elles produisent ; elles ont toutefois aussi une valeur économique. Ainsi, les entreprises utilisent désormais l'IdO pour connecter le consommateur directement au producteur. Cela permet un retour plus rapide sur la satisfaction des consommateurs et sur l'automatisation des processus de contrôle, par exemple pour des contrats de maintenance standardisés. Cette approche offre en outre la possibilité d'anticiper les tendances de consommation et les choix des consommateurs.

Le choix du produit passera dorénavant également par le choix du type de transfert et de traitement des données. Pour pouvoir jouer son rôle dans la concurrence qui va se développer entre tous les acteurs économiques, notamment dans le domaine de la « maison intelligente » (« smart home »)

⁹ IoT Analytics (2018).

Les montres intelligentes transmettent des données sensibles aux fabricants.



en anglais), le consommateur devrait être dûment informé sur de nouveaux éléments. Il importera par exemple de savoir comment les bénéfices de la collecte, de l'agrégation et de l'utilisation de données seront (re)distribués: le consommateur bénéficiera-t-il des avantages économiques liés à l'agrégation des données? Sera-t-il protégé efficacement contre les abus? En Suisse, la réforme en cours de la LPD est essentielle. Elle n'interviendra toutefois pas avant 2020 et l'on peut se demander s'il sera encore assez tôt pour infléchir les axes du développement.

Il est toutefois indispensable de mener une réflexion sur la meilleure manière d'organiser le choix du consommateur en lien avec les objets interconnectés. Doit-il avoir la possibilité de décider à qui les données seront transmises? Doit-il pouvoir disposer de plusieurs modèles? Si son véhicule est interconnecté, peut-il exiger que les données soient non seulement transmises au constructeur, mais aussi à une association privée comme le Touring Club Suisse (TCS) ou l'Automobile Club de Suisse (ACS)? En outre, il faudrait adopter des dispositifs techniques et les encadrer juridiquement afin de veiller au respect de la rétention limitée de données ou de favoriser un régime de collecte restreinte au minimum nécessaire. On ne saurait ignorer à cet égard

la mise en place d'un système de gestion collective des différends par des actions collectives et la médiation collective des différends¹⁰, comme le propose l'avant-projet de réforme du code de procédure civile¹¹.

La dimension collective des données à caractère personnel

Si l'on veut que le marché repose sur un principe de concurrence où les consommateurs peuvent jouer leur rôle, il faut probablement prendre conscience que la protection des données personnelles revêt aujourd'hui une dimension collective dont il convient de tracer les contours. En prenant des mesures pour favoriser la possibilité de choix du consommateur, notamment en lien avec la mise à disposition à des tiers des données collectées sur un objet interconnecté, on pourrait éviter que les consommateurs perdent toute maîtrise sur leurs données.

Le consentement ponctuel et binaire («oui» ou «non») n'est en effet plus en mesure d'assurer un équilibre entre utilité des données, appropriation des profits

et construction d'un régime fondé sur la confiance des utilisateurs. Il est donc temps d'appréhender la dimension plus collective des données.



Pascal Pichonnaz

Professeur de droit privé et de droit romain à l'université de Fribourg, président ad interim de la Commission fédérale de la consommation (CFC)

Bibliographie

- Commission fédérale de la consommation CFC (2015), *Recommandation du 17 février 2015 relative aux actions collectives*, Berne.
- Commission fédérale de la consommation CFC (2017), *Recommandation du 14 septembre 2017 relative à la maîtrise des données*, Berne.
- Commission fédérale de la consommation CFC (2018), *Prise de position sur le Code de procédure civile*, 7 juin, Berne.
- Conseil fédéral (2017), *Message concernant la loi fédérale sur la révision totale de la loi fédérale sur la protection des données et sur la modification d'autres lois fédérales*, 15 septembre, Berne.
- IoT Analytics (2018), *IoT 2018 in review: The 10 most relevant IoT developments of the year*, Hambourg.

¹⁰ Pour davantage d'informations: CFC (2015).

¹¹ Le texte, le rapport et le résultat de la procédure de consultation peuvent être consultés sur le site de l'Office fédéral de la justice. Voir également CFC (2018).



Pour toute la vie

Les prestations de la Croix-Rouge en Suisse

Pour en savoir plus
prestations.redcross.ch

Accompagner, soutenir, épauler. Nous sommes là.
Près de chez vous, pour vous et votre famille,
pour un monde plus humain.

Croix-Rouge suisse

