Qui est le propriétaire des données de ma santé ?

7 février 2018, 23:48 CET

Auteur Kim Boyer

Doctorante en droit de la protection sociale, Université Paris 2 Panthéon-Assas

Déclaration d'intérêts

Kim Boyer effectue sa thèse CIFRE à la Fondation d'entreprise MGEN pour la santé publique. Elle intervient lors du cycle de séminaires "les Big data en santé" organisé par l'Institut des sciences juridique et philosophique de la Sorbonne (Université Paris 1), en collaboration avec MGEN, sur la période 2017-2020.

Chacun d'entre nous produit une grande quantité de données sur sa santé, parfois même sans le savoir. Ce peut être un taux de cholestérol, après s'être rendu pour une prise de sang dans un laboratoire d'analyses ; un diagnostic de trouble du rythme cardiaque, suite à un bilan réalisé par le cardiologue ; un nombre de pas faits durant la journée, enregistré automatiquement par le smartphone.

La plupart de ces informations restent sur le papier, dans un dossier à notre nom à l'hôpital, ou dans une chemise cartonnée à la maison. Mais elles se présentent, de plus en plus, sous forme numérique. Elles peuvent être stockées sur notre ordinateur personnel ou notre smartphone mais aussi… ailleurs.

Aujourd'hui, je n'ai plus besoin de me déplacer au laboratoire d'analyses ou d'attendre le courrier pour connaître mes résultats. Il me suffit d'aller sur son site et de les télécharger. Pratique ! Seulement, mon taux de cholestérol ou de fer reste stocké sur le serveur du laboratoire. Quand je consulte un médecin dans son cabinet, le remboursement de la Sécurité sociale tombe automatiquement sur mon compte en banque, grâce à la carte Vitale. Pratique, là aussi. Mais des informations comme le nom du médecin que j'ai vu ou sa spécialité sont conservées par l'Assurance-maladie.

Ainsi, le citoyen produit des données lorsqu'il se soigne, demande un remboursement à l'Assurance-maladie ou à sa mutuelle, s'inscrit sur un groupe Facebook de patients ou se confie sur les réseaux sociaux, utilise un bracelet tracker d'activité ou un autre objet connecté pour sa santé.

Certains d'entre nous expriment une crainte, légitime, celle d'être fichés voire dépossédés de leurs données de santé. Comment partager ces informations très personnelles pour bénéficier de services profitables à notre bien-être ou encore faire avancer la recherche médicale, tout en évitant qu'elles nous échappent ? C'est l'un des sujets dont les citoyens débattent actuellement à travers les États généraux de la bioéthique.

Un « déluge » de données

Les moindres actes de notre existence s'accompagnent aujourd'hui d'une captation automatique des données, provoquant un « déluge » de données liées à notre personne. Grâce aux nouvelles technologies de l'information, combinées avec les sciences cognitives et l'intelligence artificielle, ces *big data* peuvent être organisées de manière à nous être utiles.

En ce qui concerne notre santé, les médecins et les établissements de soins ne sont plus seuls à récolter nos données. Les nouveaux acteurs, désignés comme des « collecteurs » de données, comptent notamment les géants du web comme Google, Apple, Facebook, Amazon – surnommés les Gafa. Dans la chaîne de traitement des données viennent ensuite les « hébergeurs », c'est-à-dire les entreprises détenant des parcs de serveurs informatiques pour les stocker. Enfin interviennent les *data scientists*, ou scientifiques de données, qui identifient dans la masse de données celles qui présentent un intérêt et dessinent des modèles ou algorithmes prédictifs.

Améliorer sa santé par le traitement de mégadonnées : les promesses sont immenses. Le PDG de Facebook les avait d'ailleurs évoquées en 2017, alors qu'il faisait face à des critiques sur l'aspect trop commercial de son réseau social. Dans un discours prononcé à l'université de Harvard, Marc Zuckerberg suggérait : « Pourquoi ne pas guérir toutes les maladies et demander aux bénévoles de collecter leurs informations médicales et de partager leurs génomes ? » L'idée peut paraître séduisante… mais aussi terrifiante.

Notre santé, des données personnelles « sensibles »

Au regard du droit français, les données de santé constituent des données personnelles dites « sensibles ». C'est-à-dire qu'elles méritent une protection accrue eut égard à leur nature, touchant au plus intime de l'individu. Elles sont ainsi régies par le droit commun des données personnelles, assorti d'un surplus de protections spécifiques.

Nous ne sommes pas « propriétaires » de nos données personnelles. Ce principe a été juridiquement exclu, et ce à plusieurs reprises. Ainsi, leur indisponibilité de principe a été consacrée par la loi informatique et liberté de 1978. Autrement dit, la personne ne peut en aucun cas disposer librement de ses données ni les vendre. Elle ne peut en être qu'usufruitière. En effet, la propriété est constituée de l'usus (droit d'user librement de l'objet du droit de propriété), le fructus (le droit de récolter les fruits générés par l'objet du droit de propriété) et l'abusus (le droit d'abuser de l'objet du droit de propriété, c'est-à-dire le droit de le vendre).

Plusieurs arguments juridiques sous-tendent cette position. D'abord, reconnaître à la personne « fichée » la propriété de ses données donnerait à ce droit une composante

patrimoniale. Elle aurait alors la possibilité de monnayer l'accès d'un tiers à cet élément de sa personnalité. Or les données de santé, produits du corps humain, ne peuvent pas être commercialisées par la personne. Par contre, un « collecteur » peut, lui, commercialiser un fichier de données, à condition que celles-ci soient anonymes.

Ensuite, donner un droit de la propriété à la personne fichée reviendrait à la reconnaître comme acteur principal de sa protection. Dans cette logique, elle serait la plus à même d'opérer des choix rationnels et de veiller à son propre intérêt. Ce postulat libéral est celui de la législation américaine. Mais cette position n'est pas partagée par le droit français, ni par celui de l'Union européenne.

L'un comme l'autre considèrent que la personne fichée ne peut opérer des choix pleinement éclairés. Car bien souvent elle n'est pas informée de la manière dont sera traitée l'information, ou alors de manière incomplète. Le risque est grand qu'elle sacrifie la protection de ses données personnelles pour pouvoir accéder à un service désirable. À titre d'exemple, si je veux mieux surveiller ma ligne en utilisant l'application liée à ma balance connectée, je vais entrer des données relatives à mon âge, mon poids, ma taille et bien d'autres paramètres. Et tant pis si je ne sais pas grand-chose de la manière dont celles-ci seront utilisées…

Le respect de la vie privée, mais aussi le lancement de services utiles

Les législations européenne et française ont cherché à ménager le respect des droits et libertés fondamentaux des individus, sans bloquer le flux des données à caractère personnel et les services utiles qui pourraient découler de son traitement. Elles ont institué pour cela une liberté de traitement de principe, assortie d'une police administrative spéciale.

Il s'agit à la fois de protéger les intérêts privés, autrement dit de respecter la vie privée, et de poursuivre un objectif d'intérêt général. Ce dernier consiste à pouvoir développer de nouveaux services, basés par exemple sur l'analyse de nos navigations sur le web. Des chercheurs ont ainsi proposé, dans une étude publiée en 2017 dans la revue *EPJ data science*, de diagnostiquer la dépression à partir des photos postées par la personne sur le réseau social Instagram.

Afin de défendre cette liberté de prestation de services, la communauté internationale a consacré la notion de « société d'information ». Celle-ci est issue du principe de libre circulation de l'information adopté aussi bien par l'Organisation des Nations unies (ONU), le GATT (Accord général sur les tarifs douaniers et le commerce), l'Organisation mondiale du commerce (OMC), l'UIT (Organisation internationale des télécommunications), l'Union européenne, que par le Conseil de l'Europe.

Le consentement, un droit fondamental

Toutefois, le traitement des données personnelles est conditionné à l'obtention du consentement de la personne concernée. Ce point figure dans la Charte des droits fondamentaux de l'Union européenne, adoptée en 2000, ainsi que dans une directive européenne de 1995.

Au sein de l'Union, le règlement général sur la protection des données (RGPD), signé en 2016, poursuit cet objectif d'équilibre. Il entrera en vigueur en France le 25 mai 2018. Il renforce les droits des personnes fichées en leur offrant un certain *empowerment*, mot que l'on peut traduire par la capacité à agir sur son propre destin.

L'*empowerment* passe par la libre disposition des données personnelles pour les individus, dans l'idée que chacun devienne véritablement acteur de la protection de ses droits. Aussi, les partisans du principe de libre disposition le présentent comme un rempart face à la consécration d'un droit de propriété d'acteurs extérieurs sur les données personnelles.

En France, l'adoption en 2016 de la loi pour une république numérique a anticipé sur l'entrée en vigueur du RGPD. Cette loi consacre le principe de la libre disposition. Cette dernière s'est traduite concrètement par l'assurance, par exemple, de la confidentialité des correspondances électroniques – sauf si l'usager a donné son consentement pour leur traitement automatisé.

Dans cet esprit, les individus disposent aussi d'un droit à la « portabilité » de leurs données personnelles. Celui-ci permet aux individus de récupérer celles qui sont récoltées par un prestataire de services. Ils peuvent aussi décider de les transférer à d'autres prestataires. Le but de la portabilité est de redonner aux personnes à l'origine des données un certain pouvoir sur l'usage qui en est fait. Sans pour autant qu'elles puissent les vendre.

Qui est, aujourd'hui, le propriétaire des données de ma santé ? Ni tout à fait moi-même, ni tout à fait l'organisme ou l'entreprise qui les collecte. Le législateur s'efforce de maintenir, dans la durée, un subtil équilibre entre les deux.