

Le dépouillement numérique, ou les risques liés à la quantification de l'intime

Que ce soit par le biais d'applications mobiles ou d'objets connectés comme les bracelets destinés au fitness, nous divulguons de plus en plus d'informations personnelles sur les plateformes virtuelles. Cette pratique n'est pas sans risques pour la protection des données.

Jean-Philippe Walter

Abrégé La révolution numérique s'étend désormais au secteur de la santé. Les balances intelligentes, les tensiomètres électroniques et d'autres appareils connectés permettent à chacun de mesurer ses capacités corporelles et de connaître son état de santé. Une multitude d'applications facilitent l'analyse de ces informations et leur partage avec d'autres personnes. Les données obtenues fournissent non seulement des indications sur notre forme, mais aussi sur nos habitudes et nos problèmes de santé, qui relèvent de notre sphère intime. Les compagnies d'assurances, les employeurs et bien d'autres encore sont intéressés par ces informations. Les risques pour les utilisateurs sont donc considérables.

La mesure de soi («quantified self») a connu un essor fulgurant au cours de ces dernières années. Cette approche consistant à mesurer, enregistrer et visualiser les données de son propre corps à grand renfort de capteurs et d'applications est devenue un phénomène mondial qui fascine tout à la fois les mordus de fitness, les consommateurs soucieux de leur santé et les scientifiques. Ces personnes comptabilisent leurs pas, calculent leur dépense calorique, mesurent leur tension artérielle et visualisent leurs cycles de sommeil au moyen de leur smartphone et d'outils technologiques à porter sur soi. Les fabricants lancent chaque année des produits et applications novateurs offrant de nouvelles possibilités d'utilisation. Quelque 60 millions de bracelets, montres et autres capteurs d'activité ont été vendus en 2015 – tendance en hausse. Fort logiquement, le volume de données produites suit lui aussi une courbe exponentielle.

La volonté de mieux connaître son corps grâce à des moyens techniques n'est en soi pas nouvelle, mais elle acquiert une nouvelle dimension en raison de la numérisation croissante des acti-

vités humaines. Le progrès technologique ouvre des possibilités quasi illimitées. Les appareils et applications sont connectés à des réseaux intelligents qui transmettent les informations aux serveurs des éditeurs de services. Ces données sont collectées, traitées, analysées et – dans certains cas – transmises à des tiers.

Les «bons» comportements récompensés

Plus nous utilisons d'appareils connectés et pratiquons l'auto-mesure, plus l'image qu'ils donnent de nous devient précise. L'actualité et l'exactitude des données sont d'une importance cruciale pour la qualité de l'information. La combinaison de différentes séries de mesures permet de tirer des conclusions sur notre état psychique et de détecter des maladies à un stade précoce, surtout si nous diffusons d'autres informations intimes par le biais des réseaux sociaux, de nos pérégrinations sur Internet et de nos achats en ligne (mégadonnées). De telles données répondent à

Conseils pour une utilisation sûre des objets connectés

- Réfléchissez à qui vous voulez transmettre des données sur votre corps et sur votre état de santé. La politique de confidentialité du fabricant de l'appareil ou de l'application indique à quelles fins vos données personnelles seront utilisées et si elles seront transmises à des tiers. Si cette société a son siège en Suisse, il vous sera plus facile d'exercer vos droits d'accès, de rectification, d'annulation et d'opposition.
- Configurez le service de manière à ce qu'il enregistre et communique uniquement les données nécessaires à l'exécution de la prestation.
- Il est très délicat de publier des données corporelles personnelles telles que le nombre de pas effectués, les calories dépensées, la fréquence cardiaque, etc. Utilisez un pseudonyme si vous publiez vos données sur Internet et que vous les partagez avec d'autres utilisateurs.
- Faites preuve de méfiance vis-à-vis des applications qui veulent accéder à vos contacts et à d'autres informations nullement nécessaires à la fourniture du service de base.

une forte demande, ce qui accroît leur valeur marchande. Elles intéressent en particulier les services de marketing, les employeurs et nombre d'autres acteurs.

Certaines compagnies d'assurances proposent déjà à leurs clients des applications santé et des dispositifs d'auto-mesure à porter sur soi. L'assuré qui adopte un comportement sain et accepte de livrer ses données à son assureur obtient des bons de réduction ou des rabais en contrepartie. Les capteurs de santé connaissent également un essor considérable dans le domaine du travail. Soucieuses du bien-être de leurs employés, certaines entreprises les encouragent par exemple à porter des podomètres connectés. Ceux qui obtiennent des résultats médiocres ou refusent de porter un capteur risquent-ils d'être discriminés ?

L'utilisation d'objets connectés dans le domaine de la médecine présente également certains dangers, liés d'une part à la pertinence des informations enregistrées par le patient lui-même, et d'autre part à la sécurité du stockage

des données dans le nuage et de leur transfert électronique au médecin.

Augmentation du risque d'abus

L'argument – fréquemment évoqué – selon lequel l'utilisateur intègre n'a rien à craindre perd ici de sa vigueur. Car plus nous communiquons et divulguons des données personnelles, plus la probabilité que des personnes ou des organisations mal intentionnées accèdent à ces informations est importante. Dans ce contexte, la cybercriminalité et ses multiples facettes – usurpation d'identité, cyber-intimidation, chantage, fraude – constitue un facteur à ne pas négliger.

Le droit de la protection des données repose sur la liberté qu'a l'individu de décider lui-même quand et dans quelle mesure des informations

Celui qui accepte de livrer de « bonnes » données obtient des bons de réduction ou des rabais en contrepartie.

La protection des données est difficile dans le domaine de la santé.



Les applications de smartphones et les appareils connectés mesurent, par exemple, les besoins en calories. De telles données intéressent la branche des assurances.



DEPOSITPHOTOS

relevant de sa vie privée peuvent être communiquée à autrui. Ce droit à l'autodétermination individuelle en matière d'information est toutefois privé d'effet dès lors que l'auto-mesure est érigée en norme. Celui qui – consciemment ou inconsciemment – refuse de partager ses données s'expose à des préjudices financiers ou professionnels. Il peut aussi être soupçonné d'avoir quelque chose à cacher.

Un autre écueil réside dans le fait que de nombreux services de suivi ne fournissent à leurs clients que de vagues informations sur l'usage des données collectées. Ce manque de transparence est véritablement problématique. Alors que les prestataires reçoivent une masse d'informations de leurs clients, ceux-ci ne sont pas en mesure de connaître la trajectoire et le sort réservé à leurs données. Une telle asymétrie dilue les droits des utilisateurs et crée un sentiment d'insécurité.

Il incombe aux instances politiques de fixer le cadre légal de manière à ce que les citoyens soient libres de décider si et dans quelle mesure ils souhaitent partager leurs données en matière de santé. La révision prévue de la loi sur la protection des données leur en offre la possibilité¹.

Toutefois, cette nouvelle mouture ne suffira pas à elle seule à maîtriser les risques croissants liés à la protection des données dans le contexte des nouvelles technologies, en raison notamment de la difficulté à anticiper les perspectives ouvertes par le progrès scientifique.

En outre, les utilisateurs doivent avoir les moyens de protéger de vastes pans de leur vie privée contre les regards indiscrets des entreprises et de l'État. Un travail de conscientisation est nécessaire, car un individu libre décidant, pour sa propre convenance, d'utiliser un bracelet connecté (voir *encadré*) devrait être conscient de ses responsabilités et des risques liés à la protection des données.



Jean-Philippe Walter

Préposé fédéral à la protection des données et à la transparence ad interim, Berne

¹ Le Département fédéral de justice et police (DFJP) doit soumettre au Conseil fédéral d'ici à fin août 2016 un avant-projet de révision de la loi fédérale sur la protection des données tenant compte des réformes en cours dans l'UE et au Conseil de l'Europe.