BIG DATA ET DONNÉES DE SANTÉ QUELLES RÉGULATIONS JURIDIQUES ?

ALEXANDRA MENDOZA-CAMINADE

Référence de publication : Revue Lamy Droit de l'Immatériel, Nº 127, 1er juin 2016

BIG DATA ET DONNÉES DE SANTÉ QUELLES RÉGULATIONS JURIDIQUES ?

I. - LA NÉCESSAIRE RÉGULATION DES DONNÉES DE SANTÉ EN TANT QUE DONNÉES PERSONNELLES A. - À la recherche d'une définition de la donnée de santé 1º/ La donnée de santé traditionnelle

I. - LA NÉCESSAIRE RÉGULATION DES DONNÉES DE SANTÉ EN TANT QUE DONNÉES PERSONNELLES A. - À la recherche d'une définition de la donnée de santé 2º/ La donnée de santé transmise par les objets connectés

I. - LA NÉCESSAIRE RÉGULATION DES DONNÉES DE SANTÉ EN TANT QUE DONNÉES PERSONNELLES B. - Un régime unique de protection des données personnelles

II. - LES AUTRES RÉGULATIONS JURIDIQUES ENVISAGEABLES A. - Les régulations disponibles

II. - LES AUTRES RÉGULATIONS JURIDIQUES ENVISAGEABLES B. - Pour une régulation adaptée des objets connectés ?

Le droit positif consistant en une régulation juridique sévère et complexe du *big data* en matière de santé, une réforme s'avère nécessaire afin d'établir une régulation adaptée et efficiente aux besoins de ce domaine. Tel est le sens de la présente analyse.

À l'heure du *big data*, de l'*open access* et des questions en matière de partage des données, s'interroger sur les régulations juridiques de ces phénomènes apparaît indispensable. Les effets du *big data* alliés au croisement des informations conduisent en effet à offrir des opportunités considérables pour la connaissance, la recherche et pour les activités économiques de manière générale. La santé mobile ou m-santé permet de faire apparaître un nouveau type de médecine et une évolution fondamentale du système de santé. La santé mobile a été définie par l'Organisation mondiale de la santé comme constituée des « *pratiques médicales et de santé publique reposant sur des dispositifs mobiles tels que téléphones portables, dispositifs de surveillance des patients, assistants numériques personnels et autres appareils sans fil* » (1) . Ces données de santé communiquées à travers des objets mobiles peuvent représenter de très nombreux avantages pour les citoyens ainsi que pour les entreprises. Des usages nouveaux apparaissent en dehors d'un contexte médical traditionnel, comme ceux liés aux objets dits « *connectés* » qui connaissent une croissance exponentielle tant s'agissant du marché des applications que de celui des objets connectés de santé. Le *quantified self*, nouvel eldorado économique, vise tout outil permettant la mesure de soi afin de mieux se connaître. Cette pratique conduit les personnes à livrer elles-mêmes des données de santé issues de dispositifs mobiles à des entreprises privées par le biais d'objets connectés, voire même à les partager à des fins d'information ou de comparaison, alors qu'elles ne les confiaient jusqu'à présent qu'à un médecin.

Or le *big data* est également porteur de risques pour les individus s'agissant de la protection de la vie privée en raison de la complexité et de l'opacité de ces appareils. L'utilisateur de ces objets dits « *intelligents* » a en général une conscience très limitée des questions posées par la protection des données personnelles. Ces données ainsi utilisées

semblent pouvoir échapper à toute régulation juridique et en particulier à la protection légale des données personnelles. Les risques semblent donc se multiplier à la mesure des potentialités offertes par le *big data*, et ces risques seront renforcés avec le développement de l'intelligence artificielle. Comment réguler ce phénomène et comment trouver un équilibre entre les intérêts présentés par le *big data* et les nouveaux risques qu'il est susceptible d'engendrer ? Le législateur français ne s'est pas encore saisi spécifiquement de la question et n'envisage la donnée de santé qu'au travers de la question de l'accès ouvert aux données de santé et donc de ce que l'on qualifie d'« *open access* » au travers de la loi nº 2016-41 du 26 janvier 2016 de modernisation de notre système de santé (2) . Le Conseil d'état s'est, lui, interrogé sur le cadre juridique applicable en matière de santé connectée (3) . Pour l'heure, le droit positif consiste en une régulation juridique sévère et complexe du *big data* en matière de santé, ce qui fera sans doute l'objet d'une réforme afin de répondre par une régulation adaptée et efficiente aux besoins en la matière. Ainsi, il faut tout d'abord constater que la régulation juridique essentielle des données de santé issues du *big data* intervient sur le terrain de la protection des données personnelles (I), même si d'autres formes de régulation juridique sont possibles (II).

I. - LA NÉCESSAIRE RÉGULATION DES DONNÉES DE SANTÉ EN TANT QUE DONNÉES PERSONNELLES

Le *big data* génère des données de santé innovantes et bouscule l'appréhension traditionnelle de la donnée de santé, ce qui conduit à s'interroger sur la notion de « *donnée de santé* ». Il faut en conséquence déterminer préalablement la définition de la donnée de santé (A) avant d'envisager son régime juridique (B).

A. - À la recherche d'une définition de la donnée de santé

Il est essentiel de définir et de connaître le périmètre de cette notion de « *donnée de santé* » puisqu'elle conditionne le régime juridique applicable. Or, aucune définition n'existe dans les textes applicables. La donnée en matière de santé est conçue comme une notion très large susceptible d'englober des données issues de nouveaux procédés connectés.

1º/ La donnée de santé traditionnelle

En droit, la donnée de santé est prise en compte par le législateur, et elle est inscrite dans la loi. Toutefois, cette intégration législative fut réalisée de manière récente, puisque c'est la directive nº 95/46/CE du 24 octobre 1995 (4) , transposée en droit français par la loi nº 2004-801 du 6 août 2004 (5) qui a ajouté plusieurs catégories dont les données relatives à la santé au sein des données dites « *sensibles* ». Mais cette prise en compte ne s'est pas accompagnée d'une définition légale. En particulier, la loi nº 78-17 du 6 janvier 1978 « *relative à l'informatique, aux fichiers et aux libertés* » ne donne pas de définition des données de santé. Elle se limite à définir de manière générale la donnée personnelle comme « (...) *toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement* » (6) .

Pour délimiter leur domaine, il est possible de se fonder sur la conception très large qu'en retient la Commission nationale de l'informatique et des libertés (Cnil) dans ses décisions, à savoir qu'une donnée de santé constitue toute donnée relative à la santé d'une personne ou susceptible de donner une indication sur son état de santé. Le Groupe européen des autorités de protection des données - Groupe dit « *de l'article 29* » (G29) - a précisé en 2007 que les données de santé sont des informations qui ont un lien clair et étroit avec l'état de santé d'une personne physique (7) .

Le G29 avait déjà indiqué dans un document de travail que la notion de « *données médicales* » est limitée aux données de santé ou aux données relatives à la personne (8) .

Le règlement du Parlement européen et du Conseil du 14 avril 2016 sur la protection des données propose pour la première fois une définition des données concernant la santé : il s'agit des « *données à caractère personnel relatives à la santé physique ou mentale d'une personne physique, y compris la prestation de services de soins* » (9) . L'adoption de ce règlement permet donc de consacrer cette définition large de la donnée de santé et l'on ne peut que s'en féliciter. Une telle définition permettra d'y englober un nouveau type de données de santé, à savoir les données transmises par des objets connectés.

2º/ La donnée de santé transmise par les objets connectés

Les objets connectés de santé ou de bien-être visés sont les smartphones et les matériels, dispositifs et objets de mesure personnelle, qui vont permettre ce que l'on qualifie de « *quantified self* ». Ce *quantified self* constitue un nouveau défipour les juristes en termes d'encadrement puisque ces objets intelligents du quotidien sont en relation avec l'intimité des personnes (10) . Ces objets permettent à une personne de capter des données issues de son corps ou liées à celui-ci, comme sa tension, son rythme cardiaque, pour une meilleure connaissance de soi (11) . Ils conduisent les personnes à livrer elles-mêmes des données de santé mobiles *via* internet. S'agit-il de données de santé, et le cas échéant de données de santé comme les autres ? En permettant la collecte d'informations très variées, les objets connectés portent sur des données qui ne relèvent pas toutes de la catégorie des données de santé ; ces contours flous représentent une difficulté fondamentale dans l'appréhension du *quantified self*, l'enjeu étant de déterminer le mode d'appréhension des données issues du *quantified self* et notamment au regard des exigences de la protection des données. Si de telles données peuvent être qualifiées de « *sensibles* », il suffit de les soumettre aux règles en vigueur pour des données de santé traditionnelles ; en effet, de telles données qualifiées de « *santé* » ne doivent être utilisées que dans des conditions prévues par la loi et respectueuses des droits de la personne. Pour la Cnil, il faudrait s'attacher à trois facteurs pour qualifier ces données mobiles comme étant des données de santé, à savoir le contexte médical ou non de production de la donnée, les informations objectives véhiculées par la donnée brute, et la destination des données (12) . Cette proposition conduit effectivement à identifier des données à risque qui seules méritent d'être régulées là où d'autres ne présentent aucune dangerosité pour la personne. Mais définir trop précisément les données de santé et les données sensibles au regard du *quantified self* peut se révéler inadapté et conduire à écarter des données qui *a priori* sont objectivement sans risque mais qui se révèlent signifiantes sur un plan médical, par exemple l'indice de masse corporelle qui constitue aujourd'hui un critère de détection de certains cancers. Aussi, nous considérons qu'il est dans un premier temps nécessaire d'adopter une définition large de la donnée de santé, et au besoin de confier ensuite à une autorité de régulation la mission de préciser sa teneur.

Certains états ont choisi de distinguer les données classiques traitées par les professionnels de santé des données de santé plus récentes liées au développement du *self quantified*. C'est notamment la solution adoptée par les états-Unis et la Corée du Sud (13) . Ce choix serait justifié par le fait que les données de santé liées au développement du *self quantified* relèveraient d'une logique de bien-être et non *stricto sensu* de la santé. Outre la finalité différente de ces données, l'application du régime juridique réservé aux données classiques serait inadaptée en raison de sa lourdeur et de sa complexité. Un tel choix juridique conduit à reconnaître l'existence de deux catégories de données de santé et à

potentiellement les soumettre à des régimes juridiques distincts. Cette distinction au sein des données de santé nous paraît inopportune et artificielle : en effet, selon son origine classique ou plutôt innovante, une même donnée pourrait recevoir un traitement juridique différent, alors que les dangers sont identiques pour la personne humaine. Ainsi, les objets connectés perturbent les frontières entre le domaine de la santé et celui du bien-être.

Au niveau des définitions, il est préférable de retenir une approche unitaire de la donnée de santé à l'image de la définition proposée par le projet de règlement : une telle conception indifférenciée de la donnée dès qu'il existe un lien avec la santé de la personne paraît être un élément favorisant une approche unitaire et simplifiée de la donnée de santé, ainsi qu'une approche protectrice favorable à la protection de la personne. Les données issues de dispositifs connectés de santé ou de bien-être doivent donc à défaut de précision être présumées relever de la catégorie des données de santé, afin de privilégier la sécurité juridique au bénéfice des utilisateurs. Une telle analyse permettrait d'appliquer des règles juridiques qui confortent cette approche protectrice de la personne concernée.

B. - Un régime unique de protection des données personnelles

La conception large des données de santé conduit à les englober toutes dans la même catégorie sans procéder à des distinctions. Or, par cette qualification, le régime juridique qui en découle va mettre en place une régulation susceptible d'être démesurée par rapport à l'objectif recherché. Ainsi, la donnée de santé, qu'elle soit traditionnelle ou liée à des objets connectés, est soumise à une même protection légale des données personnelles de la personne physique. Le G29 l'a d'ailleurs rappelé à l'égard des moteurs de recherche en indiquant que les acteurs du *big data* ne doivent pas se soustraire à la réglementation de protection des données personnelles (14) .

Or, la donnée de santé qualifiée de « *donnée sensible* » par le législateur est particulièrement protégée en raison de ses liens intimes avec la personne. Aussi, toute opération sur cette donnée de santé est interdite dès qu'elle permet d'identifier ou de rendre identifiable la personne concernée : il faut donc en assurer la confidentialité afin de garantir le respect de l'anonymat des patients. Le régime légal est très strict car ces données font l'objet d'une autorisation et non d'une simple déclaration. Elles font aussi l'objet d'un régime de protection spécifique au sujet de leur collecte, leur traitement et leur conservation.

Le principe est l'interdiction de collecter et de traiter les données sensibles en vertu de l'article 8-I modifié de la loi nº 78-17 du 6 janvier 1978 : « *Il est interdit de collecter ou de traiter des données à caractère personnel qui font apparaître, directement ou indirectement, les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou qui sont relatives à la santé ou à la vie sexuelle de celles-ci.* » Ce principe connaît plusieurs exceptions prévues par l'article 8-II modifié, notamment en cas de consentement exprès de la personne concernée, ou lorsque les traitements portant sur des données à caractère personnel sont rendues publics par la personne concernée, ou encore pour les traitements nécessaires à la recherche dans le domaine de la santé. Conformément à l'article 8-III, la Cnil peut également autoriser, compte tenu de leur finalité, certaines catégories de traitements « *() si les données à caractère personnel sont appelées à faire l'objet à bref délai d'un procédé d'anonymisation* ». Des droits sont prévus au bénéfice de la personne dont les données sont collectées, ainsi que des obligations à la charge du responsable de traitement.

Cet encadrement juridique très protecteur de la loi du 6 janvier 1978 s'applique ainsi à une donnée issue d'un dispositif mobile de santé pour laquelle la personne concernée aura consenti au traitement, même s'il est possible de

douter bien souvent du caractère éclairé du consentement donné par l'utilisateur. En outre, cette donnée va être partagée par l'individu avec d'autres acteurs des objets connectés. En effet, avec les outils du *quantified self*, la captation des données est réalisée directement par la personne concernée sans intermédiation d'un tiers et en particulier d'un professionnel de la santé. Cependant, divers acteurs interviennent après la captation de ces données pour les analyser. Ces tiers ne sont pas des professionnels de santé et il peut s'agir de fabricants d'objets connectés ou par exemple d'éditeurs d'applications. Les données sont donc transmises *via* internet à des sociétés privées qui ne sont pas soumises au même régime juridique que les professionnels de santé, notamment en matière de stockage et d'hébergement des données : ces divers acteurs ne sont pas soumis aux obligations des hébergeurs agréés de données de santé issues de la loi nº 2002-303 du 4 mars 2002 relative aux droits des patients (15) . Or, ces hébergeurs font l'objet d'une procédure d'agrément des hébergeurs de données de santé à caractère personnel précisée par un décret du 4 janvier 2006. Même si cette réglementation concerne les activités d'hébergement de données de santé recueillies ou produites à l'occasion d'activités de prévention, de diagnostic ou de soins, et n'est pas adaptée s'agissant de données innovantes (16) , il est important de relever qu'en matière de données issues du *quantified self*, aucune règle spécifique n'est applicable ; ce qui peut justifier des craintes quant au traitement de ces données et à leur exploitation.

Par ailleurs, un défaut d'effectivité de l'encadrement juridique existe et des garanties essentielles du droit des données personnelles ne semblent plus assurées en pratique, notamment l'obligation de confidentialité. Dans un monde interconnecté, l'anonymat des données est-il encore possible ? Le risque de réidentification de la personne à partir de données anonymes est avéré. L'évolution technologique et les procédés de *data mining* rendent la notion d'« *anonymat* » désormais illusoire et les procédés techniques d'anonymisation ne constituent plus des garanties : ce qui n'était pas à l'origine identifiant à l'égard d'une personne physique peut le devenir. Le caractère anonyme d'une donnée n'est plus aujourd'hui significatif : rapprochée d'autres données, elle peut perdre ce caractère anonyme. En effet, il suffit de croiser peu de données pour réidentifier la personne (17) , ce qui est particulièrement préoccupant en matière de santé.

Complexe et rigide, le régime d'autorisation actuellement en vigueur pour les données de santé ne semble pas adapté aux données issues de dispositifs mobiles. Toutefois, s'il faut éviter un défaut de régulation, il faudra aussi éviter un excès en matière d'encadrement des données utilisées dans le cadre du *quantified self*. Une distinction ne semble donc pas pertinente au niveau de la définition de la donnée de santé, mais une prise en compte différenciée des données dites « *traditionnelles* » et des données issues de dispositifs mobiles semble nécessaire au niveau du régime juridique.

II. - LES AUTRES RÉGULATIONS JURIDIQUES ENVISAGEABLES

Si des règles juridiques préexistantes peuvent être utilisées à ce jour, des réflexions sont en cours concernant une réglementation juridique spécifique des « *objets intelligents* ».

A. - Les régulations disponibles

Au-delà de la valorisation économique des données, une régulation peut déjà être mobilisée pour encadrer les données de santé au travers de la réglementation des dispositifs médicaux.

La valorisation économique des données de santé permet de manière classique une régulation contractuelle de ces données ainsi qu'une réservation sur le terrain des bases de données.

Dans une logique de commercialisation des données de santé, les possibilités existent aujourd'hui pour réserver l'accès à des données aux seuls cocontractants. Les contrats portant sur les données impliquent une réutilisation commerciale des données sous forme de cession de données ou de mise à disposition par un contrat de licence. L'activité de courtiers en données (*data brokers*) vise à collecter des données sur internet pour les commercialiser et les revendre à d'autres entreprises, et elle pose corrélativement la question de l'information et du consentement des personnes dont les données sont collectées. De tels contrats imposent bien sûr le respect de la législation en matière de protection des données à caractère personnel afin de protéger la personne dont les données sont ainsi exploitées.

Au-delà de la réservation contractuelle de ces données, une véritable protection juridique est offerte aux entreprises au travers du droit des producteurs de bases de données. Issu d'une directive nº 96/9/CE du 11 mars 1996 transposée par une loi du 1er juillet 1998, ce droit spécial a une fonction de protection des investissements que le producteur a réalisés pour la base de données (18) . Le droit *sui generis* permet de protéger les bases de données dont le producteur a réalisé un investissement financier, matériel ou humain substantiel au niveau de la constitution, de la vérification ou de la présentation du contenu de la base. Ce droit reconnaît au producteur le droit d'interdire une extraction et/ou une réutilisation substantielle de sa base de données par les tiers. Ces droits peuvent être transmis ou cédés ou faire l'objet d'une licence (19) . Cette protection qui organise une forme de monopole au profit du producteur conduit donc à une appropriation indirecte des données composant la base de données. Les données composant la base sont donc indirectement privatisées et protégées par le biais du droit *sui generis* des bases de données ou par le contrat qui permet leur commercialisation.

S'il n'existe aucun texte spécial pour réguler en tant que telles les données de santé, il est possible d'envisager la question de leur régulation plus largement au niveau de l'objet connecté qui intègre des données de santé. Ainsi, une régulation juridique peut intervenir sur le fondement des dispositifs médicaux.

Un dispositif médical constitue tout instrument, appareil, équipement, matière ou autre article, utilisé seul ou en association, utilisé chez l'homme pour le diagnostic, la prévention, le traitement d'une maladie, d'une blessure ou d'un handicap, ou l'étude, le remplacement ou la modification de l'anatomie ou d'un processus physiologique. Il est destiné par le fabricant à être utilisé chez l'homme à des fins médicales. Or, un tel dispositif est régi par un régime administratif strict au niveau européen.

Un objet connecté en matière de santé peut constituer un dispositif médical. En effet, cette réglementation des dispositifs médicaux peut concerner les applications de santé issues de dispositifs mobiles et les objets connectés dès lors qu'un dispositif médical vise tout appareil, équipement ou logiciel destiné par le fabricant à être utilisé chez l'homme à des fins : de diagnostic, prévention, contrôle, traitement ou d'atténuation d'une maladie, d'une blessure ou d'un handicap ; d'étude, de remplacement ou modification de l'anatomie ou d'un processus physiologique ; de maîtrise de la conception. En outre, l'action principale voulue dans ou sur le corps humain n'est pas obtenue par des moyens pharmacologiques ou immunologiques ni par métabolisme, mais dont la fonction peut être assistée par de tels moyens. Il en va ainsi des logiciels autonomes qui ne se limitent pas à stocker ou communiquer des données, mais calculent, quantifient, qualifient ou interprètent des données médicales pour le bénéfice de patients, lorsqu'ils visent spécifiquement une des actions médicales précitées.

Dans l'Union européenne, la mise sur le marché des dispositifs médicaux est soumise à plusieurs textes qui ont fait l'objet d'une harmonisation européenne se traduisant par un marquage C E (Conformité européenne). L'apposition du marquage C E est obligatoire pour de nombreux dispositifs médicaux et indique que ces produits sont conformes aux directives européennes concernant la sécurité, la santé et la protection du consommateur. Avant d'apposer le marquage C E sur un dispositif médical, le fabricant doit vérifier qu'il répond aux exigences définies dans les directives européennes concernées (réalisation de contrôles et d'essais qui assurent la conformité du produit à ces exigences). Le marquage C E garantit la sécurité d'emploi du dispositif médical et permet au produit de circuler librement dans l'Union européenne.

Les agences sanitaires nationales (en France, l'Agence française de sécurité sanitaire des produits de santé, Afssaps) interviennent, *a posteriori*, pour surveiller le marché, c'est-à-dire s'assurer de la conformité aux exigences de santé et de sécurité des dispositifs médicaux mis sur le marché sur le territoire national. Des procédures permettent d'évaluer la conformité des dispositifs médicaux, et varient selon le risque présenté par chaque dispositif. Une autoévaluation est ainsi possible pour le fabricant dont le dispositif présente un risque faible, complétée par une déclaration écrite de conformité avant d'apposer le marquage C E sur son dispositif médical. Pour les dispositifs présentant un risque plus important, un organisme est chargé de délivrer des certificats de conformité. En Europe, la réglementation des dispositifs médicaux peut protéger des objets connectés à finalité médicale. Aux états-Unis, une distinction est réalisée selon que l'objet est présenté comme un outil de traitement, de diagnostic ou de prévention d'une maladie : il est alors soumis au régime des dispositifs médicaux ; la Food and Drug Administration (FDA) contrôle les applications mobiles médicales et a autorisé une centaine d'applications considérées comme des dispositifs médicaux.

La difficulté d'utiliser le régime des dispositifs médicaux est qu'il n'existe pas de nette démarcation entre les objets soumis à ce régime et les dispositifs connectés de santé qui peuvent selon la finalité revendiquée entrer ou non dans le champ de la réglementation européenne des dispositifs médicaux. En outre, si cette régulation juridique est essentielle en termes de sécurité, elle garantit la qualité du dispositif, mais ne vise pas à assurer la protection des données personnelles collectées par un tel dispositif médical. Or, les objets connectés manquent de transparence quant au traitement des données collectées et se révèlent parfois indiscrets. D'autres régulations sont donc à envisager pour encadrer les données de santé dans le cadre du *big data*.

B. - Pour une régulation adaptée des objets connectés ?

Il n'existe pas de loi spécifique aux fins de régulation des applications du *quantified self*, mais la réflexion est dense en la matière depuis plusieurs années. Après la publication d'un livre vert, la Commission européenne a lancé une consultation sur la m-santé en avril 2014.

La Cnil a publié en mai 2014 un cahier intitulé : *Le corps nouvel objet connecté. Du quantified self à la m-santé : les nouveaux territoires de la mise en données du monde* (20) . La Cnil propose une certification des outils connectés de santé à visée médicale (21) , ce qui conduirait à écarter de la procédure de certification les dispositifs sans lien avec une maladie : dans ce cas, les applications pourraient faire l'objet d'une procédure d'enregistrement. Des restrictions d'usage des données personnelles pourraient par ailleurs être instituées en droits interne et européen afin de prévenir tout usage discriminant des données personnelles par des entreprises commerciales. L'incitation au respect de la

réglementation de la protection des données personnelles pourrait intervenir sous forme d'une labellisation au profit des entreprises.

Le groupe G29 réunissant les autorités européennes de protection des données a quant à lui adopté un avis sur l'internet des objets, le 16 septembre 2014 (22) . Le G29 a développé des recommandations pratiques pour tous les acteurs impliqués dans les objets intelligents, qu'il s'agisse de fabricants d'appareils, de développeurs d'applications, de plates-formes sociales, de plates-formes de données, d'organismes de standardisation ou encore de destinataires ultérieurs des données. Le but de ces recommandations pratiques vise à permettre aux acteurs de respecter la réglementation existante en matière de traitement des données collectées à partir de ces technologies « *prêtes à porter* ». L'avis du G29 réaffirme donc les obligations qui incombent à l'ensemble des acteurs, notamment les obligations en termes de consentement de l'utilisateur, de sécurité pour les responsables de traitement et, corrélativement, les droits reconnus au profit des utilisateurs de ces objets. Les acteurs qui se soumettraient à la réglementation en matière de protection des données personnelles pourraient alors revendiquer un avantage concurrentiel. L'utilisateur est au centre du dispositif et doit maîtriser le partage de ses données.

En France, le Conseil national de l'ordre des médecins (Cnom) a publié en janvier 2015 un livre blanc intitulé : *Santé connectée. De la e-santé à la santé connectée* (23) et préconise une régulation afin d'informer l'usager et assurant la fiabilité des technologies et la protection des données personnelles (24) . En particulier, le Cnom propose une régulation minimale par déclaration de conformité des solutions connectées de santé à des standards avec une dimension européenne ; pour apprécier la conformité, divers standards devraient être retenus, tels que la confidentialité, la protection des données recueillies, la sécurité informatique, logicielle et matérielle et la sûreté sanitaire (25) .

Dans d'autres états, des initiatives d'autorégulation ont pu être mises en place, comme au Royaume-Uni, aux états-Unis, en Espagne ou encore en Allemagne. Ainsi, le Service national de santé anglais (National Health Service) a créé un portail qui propose au grand public une sélection d'applications mobiles de santé de confiance, et une procédure d'évaluation de ces applications en fonction de leur pertinence médicale et de leur conformité à la loi sur la protection des données personnelles. Une appréciation peut donc être portée sur l'utilisation des données personnelles et aussi sur les données de santé. Les applications référencées ont été préalablement évaluées et sont classées en trois catégories : pathologies, vivre en bonne santé, information des patients. Chaque application donne lieu à une brève description. Les usagers sont également invités à communiquer leur avis (26) . En France, on peut citer la société DMD qui procède à l'évaluation d'applications mobiles de santé et formule également des recommandations (27) . Ces diverses études et initiatives ne manqueront pas d'inspirer les interventions normatives à venir aux niveaux européen et interne.

Face aux potentialités considérables du *big data*, les régulations juridiques n'en sont qu'à leurs balbutiements. Nous sommes actuellement au sein d'une période transitoire car des encadrements normatifs doivent prochainement intervenir afin d'encadrer les données issues des objets connectés. Pour l'heure, les juristes peinent à mesurer les incidences de l'utilisation et de la communication de ces données de santé tant en termes économiques qu'en termes de risques pour l'individu. Le cadre juridique actuel est sans nul doute inadapté aux nouvelles évolutions numériques car il a été conçu pour des données traditionnelles intégrées dans un environnement médical classique. Les données issues du *quantified self* ne se prêtent pas à cette appréhension juridique binaire oscillant entre la surprotection des données sensibles et l'absence de toute protection. Une brèche va donc vraisemblablement s'ouvrir au sein de notre droit de la

protection des données personnelles afin de créer une voie médiane entre l'absence de régulation et la surrégulation actuellement issue de notre dispositif légal : une catégorie de données, pourtant liées à l'intimité de la personne et potentiellement porteuses d'informations à risque, va être soumise à une protection juridique allégée. La donnée recueillie dans le cadre du *quantified self* pourrait être moins protégée en raison du contexte innovant dans lequel elle a été collectée et du fait que la personne a volontairement mis ces données à disposition et a consenti à leur captation. Pourtant, une autre solution pourrait consister à assimiler les données de santé à un élément du corps de la personne et à construire un régime très protecteur allant bien au-delà de la notion de « *donnée personnelle* » (28) . Contraint d'intervenir pour mettre en place une conception allégée de la protection des données personnelles, le législateur est donc une nouvelle fois confronté à la problématique du respect de la vie privée et de la protection du citoyen. Reste à voir quelle évolution sera choisie en France et en Europe et si elle permettra au *big data* de s'épanouir dans l'intérêt des personnes.

(1)

OMS, *mHealth New horizons for health through mobile technologies*, 2011.

(2)

Sur l'ouverture des données de santé, Castets-Renard C., Les opportunités et risques pour les utilisateurs dans l'ouverture des données de santé : *big data* et *open data*, RLDI 2014/108, nº 3605.

(3)

Conseil d'état, Le numérique et les droits fondamentaux, étude annuelle 2014, Doc. fr. 2014, voir spéc. p. 371 et s.

(4)

Dir. nº 95/46/CE, 24 oct. 1995, « *relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation des données* ».

(5)

L. nº 2004-801, 6 août 2004, « *relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel* ».

(6)

L. modifiée nº 78-17, 6 janv. 1978, art. 2.

(7)

Avis nº 4/2007 sur le concept de données à caractère personnel, 20 juin 2007, <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_fr.pdf>.

(8)

Document de travail adopté le 15 février 2007 relatif aux traitements des données à caractère personnel concernant la santé dans les données électroniques de santé : <http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/index_en.htlm>.

(9)

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 et abrogeant la directive nº 95/46/CE « *règlement général sur la protection des données* », 14 avr. 2016, art. 4 (15).

(10)

Sur la confrontation entre le droit des données personnelles et les objets connectés : Weinbaum N., Les données personnelles confrontées aux objets connectés, Comm. com. électr. 2014, nº 12, p. 14 ; voir aussi Laverdet C., Les enjeux juridiques de l'internet des objets, JCP G 2014, nº 23, p. 1154 ; Lacour S., Données de santé et numérique : foule paradoxale, revue Hommes et libertés, sept. 2015.

(11)

Gadenne E., Guide pratique du Quantified Self. Mieux gérer sa vie, sa santé, sa productivité, éd. Fyp, 2012.

(12)

Sur la définition en données de santé, voir Cnil, Le corps, nouvel objet connecté, Cahiers IP nº 02, mai 2014, <www.cnil.fr/fileadmin/documents/ La_CNIL/publications/DEIP/CNIL_CAHIERS_IP2_WEB.pdf>, p. 54.

(13)

Cnil, Le corps, nouvel objet connecté, précité, p. 45 et s.

(14)

Avis nº 1/2008 sur les aspects de la protection des données liés aux moteurs de recherche, 4 avr. 2008, <http://ec.europa.eu/justice/policies/ privacy/docs/wpdocs/2008/wp148_fr.pdf>.

(15)

Voir C. santé publ., art. L. 1111-8.

(16)

Voir C. santé publ., art. L. 1111-8, al. 1er.

(17)

Desmarais P., La réforme de l'open data suppose une approche globale !, JCP G 2014, I, 528 : trois données suffiraient pour identifier une personne physique.

(18)

Voir C. propr. intell., art. L. 341-1 et s.

(19)

Voir C. propr. intell., art. L. 342-1.

(20)

<www.cnil.fr/fileadmin/documents/La_CNIL/publications/DEIP/CNIL_CAHIERS_IP2_WEB.pdf>.

(21)

Sur la mise en place d'un tel mécanisme, voir aussi : Desmarais P., Quel régime pour la m-health ?, Comm. com. électr. 2013, nº 3, étude 5.

(22)

Voir G29, Avis sur l'Internet des objets, <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/ files/2014/wp223_en.pdf>.

(23)

<www.conseil-national.medecin.fr/sites/default/files/medecins-sante-connectee.pdf>.

(24)

Cnom, livre blanc, précité, p. 3.

(25)

Cnom, livre blanc, précité, p. 23 et 29.

(26)

Pour d'autres initiatives publiques et privées, voir : Cnom, livre blanc, précité, p. 27 et s.

(27)

<ww.dmd-sante.com>.

(28)

Voir Cnil, précité, p. 56.