”Personnalisation des soins et risques liés aux données de santé”, in: Technologies médicales innovantes et protection des droits fondamentaux des patients, C. Castaing (dir.), Mare & Martin, 2017, pp. 113-128

Rose-Marie Borges, Christine Lassalas

PERSONNALISATION DES SOINS ET RISQUES LIES AUX DONNEES DE SANTE

Rose-Marie Borges, Maître de conférences HDR, Centre Michel de l'Hospital (EA4232), Université d'Auvergne

Christine Lassalas, Maître de conférences, Centre Michel de l'Hospital (EA4232), Université d'Auvergne

La technologie a constamment ouvert de nouvelles perspectives à la médecine. Ces dernières années, le développement de la biologie moléculaire et la diminution des coûts du séquençage génétique ont permis d'intégrer les caractères génétiques du patient dans sa prise en charge. L'évolution technologique conduit à une personnalisation de la médecine, permettant de traiter chaque patient de façon individualisée en fonction de spécificités biologiques ou génétiques mais également en tenant compte de l'ensemble des facteurs pouvant influencer l'évolution de la maladie et l'efficacité du traitement (âge, état de santé, environnement, mode de vie…). Les médecins peuvent faire du "sur mesure" pour chaque patient**,** pour une plus grande efficacité de la prise en charge et une meilleure qualité de vie. C'est ainsi qu'est apparue l'idée d'une médecine personnalisée, mais le concept ne fait toutefois pas l'objet d'un consensus quant à son contenu.[1]

Notre intention n'est pas d'analyser ce concept, mais de nous focaliser sur Internet, les dispositifs mobiles et les objets connectés qui ont investi le champ de la santé et permettent une personnalisation des soins. La démocratisation des objets connectés et des applications de santé a fait naître le concept de « santé connectée » ou e-santé.

La e-santé consiste, selon l'OMS *"*à utiliser (…) les TIC à l'appui de l'action de santé et dans des domaines connexes, dont les services de soins de santé, la surveillance sanitaire, la littérature sanitaire et l'éducation, le savoir et la recherche en matière de santé." Les TIC ont été définies par l'OCDE comme une *«c*ombinaison de produits et de services qui capturent, enregistrent et affichent des données et des informations, par voie électronique ». La e-santé inclut la télémédecine et la m-santé[2].

La e-santé est présentée comme une réponse aux principaux défis auxquels fait aujourd'hui face notre système de santé : la prise en charge des personnes dépendantes, la prise en charge

[1] V. notamment M. Billaud, X. Guchet, "L'invention de la médecine personnalisée", Médecine/Sciences septembre 2015, vol. 31, n° 8-9, p. 797

[2] Pour une définition de la télémédecine, voir l'article L 6316 du Code de la Santé Publique. La m-santé a été définie par l'OMS en 2011 comme recouvrant les « p*ratiques médicales et de santé publique reposant sur des dispositifs mobiles, tels que les téléphones portables, les systèmes de surveillance des patients, les assistants numériques personnels et autres appareils sans fil*.2 », OMS, mHealth-New horizons for health through mobile technologies, Global Observatory for eHealth series, volume 3, p.6

des patients atteints de maladies chroniques, le maintien de l'égalité d'accès aux soins et l'augmentation croissante du coût de la santé.

Au-delà de l'intérêt sanitaire et économique indéniable attaché à la e santé, il convient de s'intéresser aux données personnelles qui lui sont attachées. De nombreuses données fournies par les individus peuvent être considérées comme des données personnelles sensibles qui ont besoin d'être protégées. La catégorie des données personnelles est assez hétérogène et les règles applicables varient selon la qualification attribuée aux différentes données personnelles. Nous allons donc dans un premier temps, essayer d'analyser la notion de données personnelles de santé (I) avant d'envisager les risques liés à l'utilisation du numérique en matière de données de santé, risques pour lesquels nous essaierons d'entrevoir une réponse juridique (II).

I. L'analyse de la notion de données personnelles de santé

Souvent utilisée, l'expression « données de santé » ne fait pourtant l'objet d'aucune définition. Ces données sont en principe traitées comme des données à caractère personnel bénéficiant d'un régime spécifique (A) mais, devant l'importance prise par cette catégorie de données personnelles, on assiste à une certaine autonomisation de la notion de données personnelles de santé (B).

A. Les données de santé, une catégorie de données personnelles

La donnée personnelle est définie par la loi Informatique et libertés de 1978 comme « toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne »[3].

Les données personnelles ne se résument pas aux seules informations nominatives (nom et accessoires du nom) mais englobent, depuis 2004 et les modifications apportées à la loi Informatique et libertés de 1978, d'autres éléments se rapportant à la personne, comme des images ou du son[4].

Si l'individu garde un certain contrôle sur ses données nominatives, les données personnelles le concernant échappent le plus souvent à sa maîtrise, soit parce qu'il en ignore l'existence, soit parce que la donnée d'origine a fait l'objet de transformations qui aboutissent à de nouvelles données. Ainsi, les données génétiques la concernant sont-elles généralement ignorées de la personne. De même, les traces numériques des individus sur Internet sont-elles transformées en informations comportementales permettant d'établir un profil de l'internaute.

[3] Article 2 de la l**oi** n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés

[4] Sur l'évolution du contenu de la notion de données personnelles V. J. Eynard, « Les données personnelles. Quelle définition pour un régime de protection efficace ? », Michalon 2013

Les connexions qu'a pu faire la personne sont bien connues d'elle mais donneront naissance, par recoupement, à des informations dont elle ignore tout[5].

La proposition amendée de règlement européen sur la protection des données à caractère personnel définit celles-ci comme « toute information concernant une personne physique identifiée ou identifiable ("personne concernée"); est réputée identifiable une personne qui peut être identifiée directement ou indirectement (…), notamment par référence à un identifiant, par exemple un nom, un numéro d'identification, des données de localisation, ou un identifiant en ligne, ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale »[6]. Ainsi, des données anonymisées peuvent conduire à l'identification d'une personne lorsqu'elles sont croisées avec d'autres données permettant de l'identifier[7].

Au vu de ces éléments, la donnée personnelle pourrait être définie comme « toute information saisissant par sa nature ou par son objet l'essence humaine biologique ou psychologique d'une personne physique identifiée ou identifiable et échappant intellectuellement et juridiquement à cette dernière »[8].

Les données de santé, en ce qu'elles sont intimement liées à l'individu et à sa vie privée, constituent une catégorie particulière de données personnelles. La loi Informatique et libertés de 1978 les qualifie de données sensibles, soumises à un régime plus protecteur que les simples données nominatives[9]. Au vu de cette sensibilité particulière et des enjeux économiques qu'elles représentent tant pour les opérateurs privés que publics, les données de santé tendent à devenir une catégorie autonome de données personnelles.

B. L'autonomisation des données personnelles de santé

Ni la loi de 1978, ni le code de la santé publique ne définissent les données de santé bien qu'utilisant cette expression [10]. Une première définition de la donnée de santé peut être

---

[5] *Ibid*., p. 141 s.

[6] Proposition de 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 (règlement général sur la protection des données), 11 juin 2015, 9565/15, article 4-1

[7] Pour déterminer si une personne est identifiable, il faut dans ce cas considérer l'ensemble des moyens raisonnablement susceptibles d'être mis en œuvre, soit par le responsable du traitement, soit par une autre personne (…). Il convient de considérer l'ensemble des facteurs objectifs tels que le coût de l'identification et le temps nécessaire à celle-ci, en tenant compte à la fois des technologies disponibles au moment du traitement et de l'évolution de celles-ci : Ibid., considérant n° 23

[8] J. Eynard, op*. cit.* p. 184.

[9] Constituent des données sensibles les «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» (article 8-I de la loi Informatique et libertés)

[10] L'article 8 de la loi de 1978 se contente de préciser qu'il est « interdit de collecter ou de traiter des données à caractère personnel (…) qui sont relatives à la santé ». Quant à l'article L 1111-8 CSP, il reconnaît aux professionnels de santé ou à la « personne concernée », le droit de « déposer des données de santé à caractère

trouvée dans un arrêt de la Cour de justice de l'Union européenne du 6 novembre 2003[11], la Cour qualifiant de données de santé « des informations concernant tous les aspects, tant physiques que psychiques, de la santé d'une personne ». Cette définition se base sur la définition de la santé donnée par l'OMS, selon laquelle la santé est considérée comme « un état de bien-être physique, mental et social et ne consiste pas seulement en une absence de maladie ou d'infirmité »[12].

La proposition de règlement européen sur les données personnelles définit la donnée de santé comme « toute donnée relative à la santé physique ou mentale d'une personne physique qui révèle des informations sur l'état de santé de ladite personne »[13]. Le considérant 26 de la proposition précise ce que pourrait être le contenu des données de santé : elles devraient comprendre « les données se rapportant à l'état de santé d'une personne concernée qui comportent des informations sur la santé physique ou mentale passée, présente ou future de la personne concernée, y compris des informations relatives à l'enregistrement du patient pour la prestation de services de santé (…), un numéro ou un symbole attribué au patient, destinés à l'identifier de manière univoque à des fins médicales, (…) des informations obtenues lors d'un contrôle ou de l'examen d'un organe ou d'une substance corporelle, y compris des données génétiques et des échantillons biologiques, (…) ou toute information concernant, par exemple, une maladie, un handicap, un risque de maladie, un dossier médical, un traitement clinique ou l'état physiologique ou biomédical de la personne concernée, indépendamment de sa source, qu'elle provienne par exemple d'un médecin ou d'un autre professionnel de santé, d'un hôpital, d'un dispositif médical ou d'une épreuve diagnostique in vitro ». Cette définition englobe l'ensemble des informations présentant un lien clair et étroit avec la description de l'état de santé d'une personne.

En tant que données sensibles, les données de santé sont en principe exclues de toute collecte et de tout traitement[14]. Ce principe est toutefois assorti de plusieurs exceptions, basées soit sur le consentement de la personne concernée, soit sur la finalité du traitement en l'absence de consentement.

1°) Le consentement au traitement de données de santé

Les données personnelles, notamment de santé, peuvent faire l'objet d'un traitement dès lors qu'elles ont manifestement été rendues publiques par la personne concernée[15]. La pratique du *quantified self* par exemple génère un nombre très important de données et renvoie à « un ensemble de pratiques variées qui ont toutes pour point commun, de mesurer et de comparer avec d'autres personnes des variables relatives à son mode de vie » : nutrition, exercice

---

personnel recueillies ou produites à l'occasion des activités de prévention, de diagnostic ou de soins auprès de personnes physiques ou morales agréées à cet effet ».

[11] CJCE 6 nov. 2003, Aff. C-101/01, Lindqvist, Rec. 2003, I, p. 12971, att. n° 50

[12] Préambule de la Constitution de l'Organisation mondiale de la santé, tel qu'adopté par la Conférence internationale sur la santé, New-York 19-22 juin 1946, Actes officiels de l'OMS, n° 2, p. 100

[13] Proposition de règlement sur la protection des données, *op. cit*., article 4-12

[14] Article 8 de la l**oi** du 6 janvier 1978 ; article 9-1 de la proposition de règlement européen.

[15] Proposition de règlement sur la protection des données, *op. cit*., article 9-2e

physique, sommeil…[16]. La communication de telles données par la personne concernée fait présumer son consentement. La loi peut cependant prévoir des cas dans lesquels le consentement de la personne ne suffit pas à lever l'interdiction de traitement de catégories particulières de données, dont les données de santé font partie[17].

La loi Informatique et libertés précise que le consentement de la personne à la collecte et au traitement de données de santé doit être exprès[18]. La proposition de règlement européen exige quant à elle un consentement spécifique au traitement des données de santé[19]. Ce texte distingue le consentement sans ambiguïté nécessaire au traitement des données personnelles[20], du consentement explicite exigé pour le traitement des données de santé.

Si ces termes sont généralement considérés comme équivalents, il semblerait cependant que l'intensité du consentement diffère selon l'expression utilisée. Dans tous les cas, le consentement de la personne au traitement des données doit être exprès, c'est-à-dire qu'elle doit manifester formellement sa volonté à l'acte. Le consentement non ambigu au traitement des données personnelles suppose une formalisation, écrite ou orale de cette volonté et ne saurait donc être tacite ou passif. Il vaudrait par ailleurs pour toutes les activités de traitement ayant la même finalité[21]. Il doit être suffisamment clair pour ne pas être susceptible de recevoir plusieurs interprétations. Quant au consentement explicite, il se situerait un cran au-dessus du précédent en ce qu'il ne viserait qu'une catégorie particulière de données (santé, génétiques, religieuses…) ayant une finalité déterminée. Il conviendrait dès lors de recueillir un nouveau consentement explicite de la personne dès lors que la catégorie de données ou la finalité du traitement serait modifiée.

En pratique, l'obligation pesant sur le responsable du traitement de prouver l'existence d'un consentement non ambigu ou explicite conduira à exiger un acte écrit, même si celui-ci n'est pas requis par les textes.

2°) Le traitement des données de santé en l'absence de consentement

Des dérogations à l'interdiction de traitement de catégories particulières de données sont prévues par l'article 9-2 de la proposition de règlement européen sur la protection des données. Ces exceptions rejoignent celles prévues à l'article 8 de la loi Informatique et libertés et peuvent être classées en plusieurs catégories :

---

[16] Le corps, nouvel objet connecté, CNIL, Cahiers IP n° 2, mai 2014, p. 3

[17] L'article L 1111-18 du code de la santé publique dispose que, même avec l'accord de la personne concernée, « L'accès au dossier médical partagé est notamment interdit lors de la conclusion d'un contrat relatif à une protection complémentaire en matière de couverture des frais de santé et à l'occasion de la conclusion de tout autre contrat exigeant l'évaluation de l'état de santé d'une des parties. L'accès à ce dossier ne peut également être exigé ni préalablement à la conclusion d'un contrat, ni à aucun moment ou à aucune occasion de son application. Le dossier médical partagé n'est pas accessible dans le cadre de la médecine du travail. »

[18] Article 8-II-1°

[19] Article 9-2a de la proposition

[20] *Ibid.,* Article 6-1a

[21] *Ibid.,* considérant n° 25

- Les traitements nécessaires à la sauvegarde des intérêts vitaux de la personne concernée, mais auxquels elle ne peut donner son consentement par suite d'une incapacité juridique ou physique[22] ;
- Les traitements nécessaires au respect d'une obligation légale incombant au responsable du traitement en matière de droit du travail, de la sécurité et de la protection sociale[23].
- Les traitements nécessaires à la constatation, à l'exercice ou à la défense d'un droit en justice ou chaque fois que des juridictions agissent dans le cadre de leur fonction juridictionnelle[24]
- Les traitements nécessaires pour des raisons d'intérêt public dans les domaines de la santé publique[25]. La notion de santé publique désigne l'ensemble des éléments liés à la santé à savoir l'état de santé, y compris le décès et le handicap, les éléments déterminant cet état de santé, les besoins en soins de santé, les ressources allouées aux soins de santé, l'offre de soins et l'accès universel à ces soins, les dépenses de santé et leur financement, ainsi que les causes de mortalité[26].
- Les traitements nécessaires à des fins d'archivage dans l'intérêt public ou à des fins historiques, statistiques ou scientifiques[27]

L'autonomisation des données de santé se manifeste non seulement au travers de la définition proposée par le règlement européen mais également par la possibilité pour les Etats membres d'introduire des dispositions plus précises ou restrictives en matière de données génétiques ou de données liées à la santé[28].

Les données personnelles de santé définies et leur régime juridique précisé, il reste alors à envisager les risques liés à leur collecte afin d'essayer de les prévenir.

II. Penser les risques et proposer une réponse juridique

Avec le *quantifield self*, l'individu collecte des variables relatives à son mode de vie et les partage avec d'autres personnes. Dans les quelques lignes qui vont suivre, notre démarche consistera à envisager les risques liés à la collecte et l'exploitation de ces données personnelles particulièrement sensibles (A) afin d'envisager une démarche de prévention impliquant les différents acteurs et le législateur (B).

[22] Article 9-2c de la proposition de règlement ; Article 8-II-2° de la loi Informatique et libertés
[23] Article 9-2b, 82 et 82bis de la proposition de règlement
[24] Article 9-2f de la proposition de règlement ; Article 8-II-5° de la loi Informatique et libertés
[25] Articles 9-2h, 9-2h (ter) et 81 de la proposition de règlement
[26] Article 3-c du Règlement CE n° 1338/2008 du Parlement européen et du Conseil du 16 décembre 2008 relatif aux statistiques communautaires de la santé publique et de la santé et de la sécurité au travail, JOUE L354, 31 décembre 2008 p.70
[27] Article 9-2i et 83 de la proposition de règlement
[28] *Ibid.,* Article 9-5

A. Les risques liés à la collecte de données personnelles de santé.

Il y a plusieurs façons d'envisager les risques encourus. On peut tout d'abord suivre la chaîne de traitement de l'information : les données sont collectées, puis traitées, et parfois stockées (ou hébergées). Lors de chaque transmission, il faut éviter la perte des données ou leur captation par un tiers. Il n'est nul besoin d'être un expert en informatique, pour savoir qu'actuellement il est aisé d'utiliser un logiciel *hacker* afin de visualiser, de modifier, d'ajouter ou de supprimer des données numériques.

Par ailleurs, chaque étape est susceptible d'entrainer d'autres risques. L'objet connecté est peut-être peu fiable quant à la collecte de données de santé, soit en raison d'une défaillance des capteurs ou du logiciel, soit en raison d'une tromperie sur la finalité du dispositif lui-même[29]. En effet, des données recueillies par des objets de santé « grand public », telles que des applications santé non cliniquement validées, peuvent s'avérer dangereuses pour le patient et le médecin qui les prendrait en compte dans le cadre d'un traitement médical.

Il est également nécessaire de préserver la fiabilité des données lorsqu'elles circulent. Des données peuvent être correctes mais la transmission de mauvaise qualité, entrainant ainsi des risques lors du traitement.

Un autre risque est l'utilisation des données de santé hébergées sur différents sites pour une finalité très éloignée de celle envisagée au départ. Les données collectées pourraient ainsi être utilisées pour conditionner un remboursement par la sécurité sociale[30] ou pour renseigner une assurance[31]. On voit alors poindre les risques de profilage, de discriminations sociales, de rupture d'égalité pour des individus susceptibles de déclarer telle maladie ou déjà atteints d'un cancer ou d'une maladie chronique.

On pourrait détailler davantage les risques liés au déferlement des objets connectés permettant la collecte et la circulation des données de santé. En réalité, c'est toute une économie qui s'est construite autour des données de santé. L'exploitation des données personnelles de santé présente en effet un intérêt majeur pour la médecine mais également pour de nombreux acteurs dont le modèle économique repose sur l'exploitation du *Big Data*, c'est-à-dire de très

---

[29] Des applications peu fiables peuvent donner aux utilisateurs un sentiment de sécurité quant à une maladie, un traitement (existence ou non de lésions cutanées, traitement de l'hypertension…), et entrainer un retard dans les traitements, une perte de chance. Pour des exemples, V. notamment « Santé connectée », Le Livre Blanc du Conseil National de l'Ordre des Médecins, Janvier 2015, p.22 s.

[30] Ainsi, il est possible de détecter l'apnée du sommeil par des capteurs connectés, des applications mobiles qui évitent au patient de séjourner à l'hôpital. En 2014, le Conseil d'État (CE, 28 novembre 2014, Union nationale des associations de santé à domicile et autres) a annulé les arrêtés du 9 janvier et du 22 octobre 2013 modifiant les modalités de remboursement par l'assurance maladie du traitement de l'apnée du sommeil. Ces deux arrêtés subordonnaient notamment la prise en charge du coût du traitement à l'utilisation effective d'un dispositif médical. L'utilisation de l'appareil était contrôlée par un dispositif de transmission automatique des informations.

[31] « Il faut ajouter à cela que l'activité des *data brokers* (courtiers en données) est en plein développement. Ces sociétés se spécialisent dans la récolte d'informations de consommation, à partir de sources en ligne et sans que le consommateur ne soit au courant, pour les revendre à des entreprises, banques ou assurances… » *in* Santé connectée, précité, p.21 ; Basini B., Les données personnelles, l'or noir du XXIème siècle, http://www.lejdd.fr/Economie/Les-donnees-personnelles-l-or-noir-du-XXIe-siecle-764003 (consulté le 13 février 2016)

grands volumes de données. Le *Big Data* est à la source du développement de nombreuses sociétés organisées autour de la monétisation des données[32], car une fois collectées, elles représentent une valeur marchande. On peut donc s'étonner de la légèreté avec laquelle les usagers confient leurs données de santé, plus ou moins fiables et intimes, données qui vont pouvoir être exploitées.

Fournies volontairement ou non, consciemment ou non, à un gestionnaire de bases de données plus ou moins identifié, les données circulent ou peuvent potentiellement circuler. D'où la nécessité de réguler et d'envisager des outils pour protéger les données ainsi que les individus à l'égard des traitements que l'on peut faire de leurs données personnelles de santé[33].

B. La prévention des risques liés à la collecte et aux traitements des données de santé.

La prévention des risques passe à la fois par la protection des données dès la conception ou l'élaboration d'un objet ou d'un service (1°) ainsi que par une plus grande implication des utilisateurs d'objets connectés (2°) et une véritable prise en compte du caractère mondial des flux de données (3°).

1°) La protection des données dès la conception des objets ou des services

« Les objets connectés sont des passoires en matière de sécurité »[34], aussi convient-il de se demander comment remédier à cet état de fait, d'autant plus que beaucoup de données personnelles de santé transitent par le réseau Wi-fi peu sécurisé. La solution semble être d'installer des filtres intégrés aux objets connectés, afin d'assurer le cryptage, voire l'anonymisation des données collectées, dès la fabrication de l'objet connecté. Il faudrait également que ces objets intègrent dès leur conception, un procédé permettant d'assurer la suppression des données. Elles concrétiseraient ainsi le droit à l'oubli, à l'effacement des données[35]. Des risques seraient évités si un certain niveau de sécurité pour que l'objet puise être commercialisé et utilisé était imposé par le législateur.

Cette approche a été retenue dans plusieurs articles de la proposition de règlement relatif à la protection des données à caractère personnel[36]. Elle est clairement exprimée au considérant 61 : « […] Lors de l'élaboration, de la conception, de la sélection et de l'utilisation

---

[32] Sur les différents modèles économiques sur le marché de la santé mobile et l'utilisation des données, voir notamment « Le corps, nouvel objet connecté », CNIL, Cahiers IP n° 2, *op. cit.* p. 28

[33] Pour reprendre une formule utilisée *in* CNIL, Cahiers IP n°1, Vie privée à l'horizon 2020, p. 46

[34] Selon le titre d'un article de 01net, août 2014, http://www.01net.com/actualites/les-objets-connectes-sont-des-passoires-en-matiere-de-securite-624818.html (consulté le12 février 2016)

[35] Le droit à l'oubli n'a pas encore été consacré par la loi ; la loi informatique et liberté (article 40) envisage un droit à l'effacement des données personnelles ainsi que le projet de règlement européen relatif à la protection des données personnelles (article 17). Enfin, actuellement, il y a un conflit entre la CNIL et Google à propos du droit au déréférencement (voir *in fine*).

[36] Proposition de règlement sur la protection des données, *op. cit.,* Articles 23, 30, 32a, 33a et 33

d'applications, de services et de produits qui se fondent sur le traitement de données à caractère personnel ou traitent des données à caractère personnel pour remplir leurs fonctions, il conviendrait d'inciter les fabricants de produits, les prestataires de services et les producteurs d'applications à prendre en compte le droit à la protection des données lors de l'élaboration et de la conception de tels produits, services et applications[…]. ».

Cette démarche de protection des données dès la conception, ou *privacy by design*[37] concerne non seulement la conception des objets connectés, mais aussi les services, les programmes de collecte, de traitement, de conservation des données. Bien appréhendée par les sociétés innovantes, elle peut constituer un facteur de « différenciation concurrentielle » : offrir un produit ou un service qui inclut la protection juridique des données personnelles de santé, permet de se différencier aux yeux des consommateurs et constitue un avantage certain.

Une telle démarche pourrait faire l'objet d'une labellisation ainsi que le préconise la CNIL. Depuis septembre 2011, elle peut délivrer des labels permettant d'identifier et donc de privilégier les organismes qui garantissent un haut niveau de protection des données personnelles[38]. Cela suppose bien entendu d'établir des référentiels. Des systèmes de certification existent déjà en la matière, dans certains pays européens ainsi qu'aux Etats-Unis[39].

Si la diminution des risques liés à la collecte et au traitement des données de santé connectées passe nécessairement par une action sur les technologies utilisées, les utilisateurs ont aussi un rôle essentiel à jouer.

2°) Le rôle des utilisateurs d'objets connectés

Nous avons vu que les données personnelles de santé peuvent être collectées avec le consentement de la personne. Il convient donc de s'assurer que le consentement a bien été donné, ce qui peut se révéler délicat. En effet, le consentement est généralement formalisé par un écrit ou une case à cocher, pour des raisons de preuve notamment. Mais en matière d'objets connectés, faut-il considérer que le simple usage vaut consentement ?

De plus, le consentement doit être spécial et même explicite si l'on s'en tient aux termes de la proposition de règlement européen[40]. Le risque est qu'en pratique, par manque d'informations ou par manque de lisibilité, il ne s'agisse pas d'un choix éclairé. Ainsi, on peut légitimement s'interroger sur le consentement donné par les utilisateurs de bracelets connectés, de piluliers, de tensiomètre ou de tout autre objet connecté. Ont-ils donné leur consentement pour que les

---

[37] Celui-ci est parfois présenté comme un frein à l'innovation car incompatible avec le *Big Data*, mais rien n'est moins certain. Voir notamment « Les données numériques : un enjeu d'éducation et de citoyenneté », CESE, janvier 2015, p. 90.

[38] Le pouvoir de labellisation de la CNIL découle de l'article 11 3 c de la loi du 6 janvier 1978 modifiée, il en existe 4 actuellement. Sur ce point, V. le site de la Cnil et la fiche pratique du 2 octobre 2015 concernant les labels ainsi que http://www.ticsante.com/la-Cnil-envisage-de-labelliser-les-applications-de-sante-mobile-NS_1868.html (consulté le 12 février 2016)

[39] V. notamment Le Livre vert sur la santé mobile, Commission Européenne, 2014, p. 13.

[40] Voir *supra*

données soient enregistrées et traitées et si oui, pour quelles finalités ? Reconnaitre une obligation de loyauté renforcée permettrait d'engager la responsabilité de ceux qui se livreraient à un traitement des données dont la finalité ne correspond pas à celle voulue au départ.

Par ailleurs, il conviendra de déterminer à qui revient le rôle d'informer. Informer prends du temps or les médecins en manquent souvent. Ce n'est donc peut-être pas à eux d'expliquer à leurs patients comment fonctionne l'application santé installée sur leurs téléphones.

A côté des traitements proposés par les médecins, encadrés par le système de santé tel que nous le connaissons, et pour lesquels se posera déjà la question du consentement du patient, les objets connectés font intervenir d'autres acteurs : les *start up*, les sociétés d'hébergement… Les questions liées au consentement de l'utilisateur de l'objet connecté ainsi que celle de la préservation de la confidentialité des données se posent alors de manière accrue.

En outre, la collecte d'informations relatives à la santé va inéluctablement conduire au traitement de données sans le consentement éclairé des utilisateurs. A titre d'exemple, nous pouvons nous interroger sur l'accord passé entre 23andMe, un laboratoire américain cofinancé par Google et une filiale du groupe Roche, Genentech, concernant la recherche contre la maladie de Parkinson. La société 23and Me a vendu des *kits* salivaires à des personnes souhaitant connaître leur patrimoine génétique. Les données personnelles anonymisées ainsi collectées ont ensuite été vendues au laboratoire Genentech, pour les utilisateurs ayant accepté. La société 23andMe a donc fait de gros bénéfices en vendant les *kits* salivaires et elle les a considérablement augmentés en vendant les données à Genetech. Or, « le bon sens voudrait que ce soit la firme qui paie pour obtenir des données de ses clients »[41]. Et l'on peut se demander quelle information a été délivrée aux utilisateurs du *kit* salivaire concernant la collecte, l'utilisation et le traitement des données de santé collectées initialement par le vendeur.

Il est donc essentiel de réfléchir dès à présent aux moyens d'éduquer les citoyens que nous sommes à l'utilisation d'objets ou d'application mobiles.

3°) La prise en compte par le Droit des flux mondiaux de données

Pour protéger les données personnelles relatives à la santé, il est possible de reconnaître de nouveaux droits et devoirs : devoir de loyauté des hébergeurs, droit de propriété de l'utilisateur sur ses données personnelles, droit à l'oubli afin d'obtenir la suppression des données, droit à l'autodétermination… Cela ne suffira cependant pas en raison du caractère mondial de la circulation des données. Il n'existe actuellement aucune norme et aucun organisme international qui peut réguler internet et le *Big data* au niveau planétaire. La CNIL, saisie par des internautes, en a fait l'expérience lorsqu'elle a demandé à Google de procéder

[41] A. Nieto, « « Santé » et « *Big data* » : Google à l'origine d'une nouvelle ère d'encadrement des données personnelles de santé ? », Revue Droit et Santé, n°67, p.649,

au déréférencement de pages et de supprimer certains liens, en se basant sur une décision de la Cour de justice de l'Union européenne du 13 mai 2014[42] reconnaissant le droit au déréférencement. Google a procédé au déréférencement « sur les extensions européennes du moteur de recherches (.fr ; .es ; .uk ; *etc.*) » mais n'a pas obtempéré pour « les autres terminaisons géographiques ou sur google.com, extensions que tout internaute peut consulter alternativement ». L'autorité de la décision de la CJUE se limitant au territoire européen, Google a fait savoir qu'il refusait d'effectuer le déréférencement sur les extensions « .com ». La CNIL a alors mis en demeure la société Google de procéder au déréférencement sur toutes les extensions et l'a condamné à 100000 euros d'amende en mars 2016. La principale difficulté concerne l'application territoriale du droit. Selon la CNIL, sa décision « ne traduit pas une volonté d'application extraterritoriale du droit français (…). Elle se borne à demander le plein respect du droit européen par des acteurs non européens offrant leurs services en Europe »[43].

En conclusion, le législateur peut protéger les données de santé ou plus précisément « la souveraineté de l'individu sur ses données »[44], en affirmant l'existence de droits et de devoirs : droit à l'oubli, droit au respect de la vie privée, devoir de loyauté de l'hébergeur… Mais cela semble dérisoire car ces droits ne sont pas inscrits dans le droit objectif de tous les Etats et le *data* n'est pas cantonné à un pays ou un territoire déterminé. Peu de solutions semblent envisageables. On peut imaginer une meilleure coopération entre les Etats, au sein d'organisations internationales ou par le biais d'accords multilatéraux, mais cette évolution relève pour l'instant de l'utopie.

Il semble donc qu'une protection véritablement efficace passe par la technologie avec le *privacy by design*, par des services sécurisés grâce à des programmes de cryptage ou de tatouage numérique, par des applications sécurisantes et surtout, par l'implication des utilisateurs.

---

[42] Affaire C-131/12, arrêt Google Spain http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&pageIndex=0&doclang=fr&mode=lst&dir=&occ=first&part=1&cid=343572 (consulté le 12 février 2016)

[43] Voir CNIL, http://www.cnil.fr/linstitution/actualite/article/article/droit-au-dereferencement-rejet-du-recours-gracieux-forme-par-google-a-lencontre-de-la-mis/ (consulté le 12 février 2016)

[44] Selon les propos de P.-O. Gibert, cité par la CNIL, Cahiers IP n°1, Vie privée à l'horizon 2020, p. 46.