Thomas Roche

La santé, une donnée très connectée

Les technologies de l'information modifient en profondeur la manière dont on aborde aujourd'hui la santé. Et les données de santé sont au cœur de ce mouvement de fond qui tend vers une médecine personnalisée : de la télémédecine aux applications d'auto-évaluation, en passant par les logiciels de santé et le big data. Thomas Roche, avocat spécialisé dans les sciences du vivant, nous expose la problématique juridique de la donnée de santé, donnée sensible dont le périmètre n'est pas clairement défini. Il évoque aussi les conséquences de l'application du statut de dispositif médical aux logiciels mais aussi son point de vue sur la libéralisation des données de santé, telle qu'envisagée par le projet de loi sur la santé.

Sylvie Rozenfeld : Avocat associé du cabinet Delsol, responsable du département Sciences du vivant, vous vous intéressez aux développements des technologies de l'information en matière de santé. La loi du 6 janvier 1978 n'avait pas intégré la donnée de santé au nombre des données sensibles. Aujourd'hui, elle figure dans la loi de 2004 et elle est aussi devenue un nouvel El Dorado. Il existe aujourd'hui plus de 100 000 applications mobiles liées à la santé. Le sujet préoccupe les professionnels du secteur. Le Conseil national de l'ordre des médecins vient de sortir un livre blanc sur la santé connectée, la Commission européenne sur la santé mobile. L'exemple le plus courant est le quantified self, ou l'auto-évaluation : 70% des applications se rapportent au bien-être et 30% sont destinées aux professionnels de santé. A partir de quel moment a-t-on affaire à une donnée de santé ? Le nombre de pas en est-elle une ?

Thomas Roche : Il n'y a pas de définition précise de la donnée de santé. La loi Informatique et libertés se contente de dire que la donnée de santé est une donnée sensible. On a quelques éléments dans le code de la santé publique, notamment l'article qui concerne l'hébergement des données de santé. En l'occurrence, ce sont toutes les informations liées au soin, au diagnostique, à la surveillance, etc. qui seront récupérées par un service de santé.

Il y a donc la donnée en elle-même et sa destination.
Plus précisément, c'est la donnée sur la personne dans le contexte de sa récupération. On parle bien d'une donnée récupérée dans le cadre du suivi d'un patient par un professionnel de santé. A contrario, une information qui serait obtenue directement par la personne ne serait pas une donnée de santé.

Et en dehors d'un parcours de soin, qu'en est-il de la transmission d'informations à partir d'un objet connecté ?
Dans ce contexte, l'information n'est pas recueillie par un professionnel de santé mais par un objet connecté qui produit de l'information grâce à des capteurs. Cet objet enregistre un état physiologique (poids, nombre de pas, cycles du sommeil, etc.). Cette information collectée par un smartphone ou une application embarquée sur un objet connecté est envoyée à un site web que la personne peut éventuellement consulter, de façon plus ludique et plus lisible. Elle peut aussi les consulter sur son smartphone, mais ces informations sont, la plupart du temps, transférées, ne serait-ce que pour les conserver. Les fournisseurs d'applications mettent en avant le fait qu'en cas de problème sur l'appareil, l'information n'est pas perdue. Ces indicateurs biologiques ou physiologiques de la personne sont à un moment donné associé à un identifiant. Il est donc possible de savoir à qui appartient cette information. Nous avons donc affaire à une donnée directement ou indirectement personnelle.

« Une information a priori anodine peut être sensible. »

La donnée est personnelle mais elle n'est pas toujours sensible.
Exactement. Les données sur les pas d'une personne ne sont pas des données sensibles car elles ne sont pas en lien avec l'état pathologique de la personne. Donc l'autre élément qui permet de caractériser une donnée de santé est le fait de savoir si cette information nous donne une indication sur le l'état pathologique de la personne.

Santé = pathologie ?
Exactement. C'est une interprétation restrictive de la donnée de santé issue de plusieurs sources. Quand on prend notamment le considérant 26 du projet de règlement européen sur les données personnelles, on retrouve cette notion liée à l'état pathologique de l'individu. Si des éléments permettent de déterminer que la personne a des problèmes cardiaques, on peut considérer que les informations liées à son pouls, etc. sont des données de santé.

Si ces éléments permettent de conclure qu'elle n'est pas cardiaque, ce ne sont donc pas des données de santé ?
C'est toute la problématique. Une information a priori anodine peut être sensible. Si la personne prend son pouls quand elle court, ce n'est pas une information sensible. Si elle effectue ce contrôle car elle sait qu'elle a un problème cardiaque, on peut estimer qu'il s'agit d'une donnée de santé dans la mesure où une décision thérapeutique peut être prise à partir de cette donnée. C'est la raison pour laquelle il n'y a pas de définition précise de la donnée de santé car il faut s'adapter au cas par cas et à chaque personne. Par ailleurs, on ne peut pas s'intéresser à la problématique des données de santé sans évoquer la télémédecine. La télémédecine constitue un acte médical et elle est réservée aux médecins. Il y en a plusieurs types : la télésurveillance, le télédiagnostique, etc. La télémédecine peut nécessiter de recourir à de telles applications, à des dispositifs médicaux pour faire remonter l'information vers le médecin afin qu'il puisse surveiller à distance l'état de santé de l'un de ses patients. Si l'on considère qu'il s'agit d'une donnée de santé, celle-ci est protégée par le code de la santé publique. Le médecin n'a donc pas le droit de la divulguer. Le secret garantit la protection de la vie privée des personnes. Si la personne veut divulguer une telle information, elle doit savoir à quel risque elle s'expose.

Peut-on appliquer la définition des données de santé, telle que celle figurant dans le texte sur les hébergeurs de données de santé, aux informations collectées par les applications de quantified self ?
Certains souhaitent qu'il y ait un élargissement de la notion de données de santé, telle qu'on la retrouve dans la définition de l'article 1111-8 du code de la santé publique, dans le cadre des hébergeurs de données de santé, afin d'y englober toutes les données physiologique et biologique sur une personne. De sorte que seuls les hébergeurs seraient habilités à les conserver. Aujourd'hui, on ne sait pas ce que les éditeurs d'application font de ces données.

Est-ce la position des seuls hébergeurs ?
Bien sûr, ils sont directement concernés car cela provoquerait un élargissement considérable de leur marché. Des médecins pourraient considérer qu'avec le développement du big data, des informations en apparence anodines pourraient devenir sensibles. L'exploitation de données massives va, à terme, nous permettre de déduire certaines pathologies. Il serait souhaitable de mettre en place des mesures de sécurité adéquates pour s'assurer au final que ces données soient correctement protégées.

Sauf qu'une donnée stockée chez un hébergeur de données de santé représente un coût supplémentaire. Cela convient-il aux petites applications de bien-être ?
Mon réel souci est que la personne concernée soit réellement informée de l'utilisation qui est faite de ses données. De complexifier les contrôles ou d'élargir la définition de données de santé pour y faire entrer beaucoup d'informations peut, au contraire, se révéler contre-productif, bloquer certains développements, voire des innovations. Je pense que le système actuel fonctionne bien. En fonction de chaque situation et les éléments dont on dispose, on arrive à déterminer si on a affaire à des données de santé ou non. En cas de doute, on retient la qualification de donnée de santé pour garantir une sécurité juridique. Cela peut avoir une incidence sur le produit qui peut être considéré comme un dispositif médical, ce qui induira aussi d'avoir recours à un hébergeur agréé, etc.

« Mon réel souci est que la personne concernée soit réellement informée de l'utilisation qui est faite de ses données. »

Pour Thierry Sirdey directeur général adjoint de l'Agence nationale de sécurité du médicament et des produits de santé, « ce n'est pas l'usage qui fait le statut d'une application, mais la destination de l'usage faite par le fabricant », qu'en pensez-vous ?
C'est exactement la définition donnée par la directive européenne 93/42/CEE modifiée sur les dispositifs médicaux. Pour arriver à déterminer si un logiciel ou un appareil est un dispositif médical, on regarde la destination qui lui est assignée par le fabricant. L'ANSM (Agence nationale du médicament et des produits de santé) vient d'apporter une illustration de l'interprétation de cette notion de dispositif médical dans une décision de police sanitaire du 12 janvier dernier. Il s'agit d'un logiciel qui permet aux personnes de conserver des informations sur leur santé, une sorte de carnet de santé numérique. Cette décision nous dit que le logiciel qui permet de recueillir de la donnée de santé n'est pas un dispositif médical. En revanche, sera considéré comme tel le module de cette solution qui permet de compresser et d'analyser une image de type radio ou autres à des fins de diagnostic. Il le sera car le fabricant aura prévu la lecture de la radio grâce à ce module. L'ANSM en a conclu qu'il s'agit d'un dispositif médical de classe IIa en fonction de la grille de classification qui comprend : I, IIa, IIb et III. Selon la classification, il y aura un process de validation pour pouvoir apposer le marquage CE sur le produit. Dans cette affaire, l'ANSM a décidé de retirer le logiciel du marché jusqu'à une mise en conformité. Cette décision administrative vient illustrer la définition du logiciel en tant que dispositif médical. C'est décision est une première extrêmement importante.

La démarche est-elle lourde pour obtenir ce marquage CE ?
Il ne faut pas se tromper de marquage CE. Certains produits vont en avoir un. Mais il ne s'agit pas de celui des dispositifs médicaux mais de celui pour les appareils électriques. Pour le marquage CE des dispositifs médicaux, la procédure est assez lourde. Le fabricant entre dans le cadre d'un vrai statut réglementé, et devient opérateur du secteur de la santé avec des obligations spécifiques. Quand on met un tel produit sur le marché, on doit, en fonction de sa dangerosité, le déclarer à l'ANSM et mettre en place tout un système de matériovigilance. Il faut démontrer que la conception et la fabrication permettent d'arriver à un produit fiable et sûr. Si un logiciel n'est pas bien calibré, paramétré, la donnée collectée peut être « sale » et elle produira des résultats non exploitables.
Quand on développe un logiciel qui est un dispositif médical, on a une série de normes à respecter. Il faut faire la démonstration de la sécurité d'emploi d'un produit, qui a été testé. Plus l'impact sur la santé est important, plus l'éditeur doit multiplier ces tests pour démontrer la robustesse du programme et respecter toute une série de normes pour obtenir le marquage CE. Un médecin peut engager sa responsabilité s'il préconise un produit qui n'a pas ce marquage. Outre la qualité du produit, le résultat peut ne pas être fiable si l'utilisateur place mal les capteurs. Par ailleurs, pour utiliser un tel produit chez lui, l'utilisateur doit être formé et clairement informé des conditions dans lesquelles les données doivent être captées.
Dès qu'un dysfonctionnement d'un appareil peut causer un préjudice à un patient ou un professionnel de santé, on doit en informer l'ANSM et mettre donc en place cette matériovigilance. Il y a par ailleurs des contraintes en matière de publicité. Certaines sont interdites dans la presse et sur internet. Cela oriente donc le marché auquel on s'adresse. S'il s'agit d'un dispositif médical, le marché sera plus petit et aussi plus contraignant. Et cela a des incidences en termes de coûts.

Les développeurs d'application pour objets connectés sont en général des petites structures qui n'ont probablement pas idée de ces obligations. Et la plupart des produits sont destinés au bien-être. Est-ce qu'il y a des applications d'auto-évaluation qui sont entrées dans ce cadre ?
Il y en a. Et certaines applications peuvent être considérées comme un dispositif médical. L'application, c'est un logiciel. Et s'il est présenté par son fabricant avec une finalité en lien avec le soin, il peut être potentiellement considéré comme un dispositif médical.

Il faut vraiment être dans le milieu de la santé pour connaître cette réglementation.
Un certain nombre d'opérateurs vont le découvrir. L'ANSM a indiqué à la fin de 2014 qu'elle allait s'intéresser aux logiciels. Cette décision du 12 janvier 2015 est sans doute la première d'une série. L'Agence va regarder de près ces produits, leur destination, leur utilisation, etc. Donc concrètement, sera considéré comme un dispositif médical une app qui collecte un certain nombre de données, de santé ou non, sur une personne ce qui va peut-être permettre d'affiner un diagnostic par un professionnel de santé ou lui faire privilégier telle solution thérapeutique par rapport à une autre.
A contrario, on voit des éditeurs d'application de quantified self se positionner sur le marché du bien-être, volontairement pour que le produit ne soit pas considéré comme un dispositif médical. Car ils savent qu'ils auront des contraintes sur la promotion, la commercialisation, le suivi, qui ne seront pas celles du marché grand public. Le rôle des professionnels est de permettre au public de voir clair dans ce marché, de l'informer et de le rassurer sur la réelle portée de tel ou tel dispositif pour qu'il n'y ait pas de confusion et de conséquences dommageables.

Des logiciels de qualité mais utilisé dans de mauvaises conditions ou avec des capteurs peu adéquats peuvent provoquer des dommages. Comment déterminer les responsabilités de chacun ?
Le jour où il y aura des problèmes de ce genre, on aura des dossiers de responsabilité fort intéressants, avec des expertises passionnantes. On imagine que chacun des intervenants se renverra la balle : la connexion entre le capteur et le logiciel qui va être analysée, le logiciel en lui-même qui peut avoir boggué, l'analyse des résultats qui peut ne pas avoir été faite correctement par le professionnel de santé ou la personne, etc.

« En cas de doute, on retient la qualification de donnée de santé pour garantir une sécurité juridique. »

Ces questions ne sont-elles pas résolues par le contrat ou les conditions générales d'utilisation ?
Ça peut l'être. Mais tout le travail d'un avocat sera de démontrer que l'éditeur ou le vendeur du produit n'a pas respecté la réglementation et n'a pas qualifié correctement son produit ou logiciel. C'est donc pénal.

Pour ces produits de quantified self, existe-t-il une certification ?
Non mais je pense qu'aujourd'hui, la priorité est de se concentrer sur l'information. Le consommateur doit pouvoir savoir si le produit va lui apporter une vraie information, ou s'il s'agit d'un gadget. Entre l'absence de toutes mentions et de marquage CE, il pourrait y avoir un niveau intermédiaire d'informations obligatoires. C'est la démarche entreprise aux Etats-Unis avec cette obligation d'informer la FDA, la Federal Drug Administration, lors de la mise sur le marché d'une application qui est en lien avec la santé.

La certification de toutes les applications paraît impossible, vu la lourdeur. Le rapport du Cnom préconise plutôt une déclaration de conformité à des pré-requis techniques. Qu'en pensez-vous ?
C'est un peu ce qu'on va retrouver avec les dispositifs médicaux. Il y a plusieurs classes. Pour la classe I qui correspond à des produits peu dangereux, une auto-certification est demandée au fabricant, sur la base d'un certain nombre d'éléments, à savoir la confirmation du respect des « exigences essentielles » en termes de sécurité et de performance. Dans ces conditions, il peut apposer le marquage CE sur son produit. Pour les classes IIa, IIb et III, il faut se tourner vers un organisme certificateur indépendant.

Pourrait-on imaginer que la Cnil élabore un cadre pour une labellisation ?
Ce ne serait pas une mauvaise idée. Cela procurerait un minimum de garantie sur l'information des personnes quant au traitement des données et leur exploitation. Ce serait une sorte de garantie de l'opérateur et un signe de sérieux de l'application. Il y a un exemple très proche de celui-ci en matière de logiciels d'aide à la prescription et à la dispensation, à destination des professionnels de santé. La Haute autorité de santé a accrédité un organisme qui peut labelliser les éditeurs de logiciels, à compter du 1er janvier 2015. Dans les caractéristiques de ces logiciels, il doit y avoir des bases de données complètes et à jour de médicaments. L'idée est d'avoir un outil d'assistance qui va donner de l'information fiable. Il y a tout un protocole de tests, avec des situations fictives pour voir comment réagit le logiciel. Un organisme certificateur, mandaté par l'HAS, va examiner le logiciel pour le compte de son éditeur.
Cette idée se retrouve dans le projet de loi de santé par rapport aux opérateurs qui vont pouvoir faire des études épidémiologiques à partir des données de santé. Le texte prévoit un process qui vise à certifier les personnes qui vont pouvoir mener ce genre d'études et faire de la recherche. La Cnil va délivrer ces accréditations. Si on revient sur les applications de quantified self, pourquoi ne pas imaginer qu'un organisme puisse s'assurer que les données collectées par une application, via un smartphone ou autre, soient traitées en conformité avec la législation ? D'une certaine façon, c'est aussi le rôle des Cils en entreprise ou du futur DPO (Data privacy officier) prévu par le futur règlement européen. Il va devoir faire la démonstration de cette analyse préalable du respect de la protection des données personnelles.
Du point de vue de l'utilisateur d'une application, la vraie question qui se pose est l'utilisation de ses données. Il n'a pas vraiment d'idée de l'activité commerciale générée par la collecte de ses données, il pense éventuellement qu'elles restent stockées sur son téléphone.

A qui profite le quantified self ? Est-ce à la personne ou aux opérateurs qui stockent ces données ?
L'information est récupérée et les fichiers peuvent être revendus. Rappelons-nous que nous avons affaire à de l'information biologique ou physiologique, voire des données de santé. Si on fait des recoupements de fichiers, on peut en déduire un profil. On peut imaginer le pire des scénarios, à savoir que ces données soient vendues à des banques ou des assurances pour sélectionner les clients. A priori, ce n'est pas encore le cas.

Les données peuvent être utilisées comme statistiques pour en déduire des tendances. Même si elles sont anonymisées, on sait aujourd'hui qu'en croisant des fichiers, on peut les repersonnaliser.
On m'a assuré qu'effectivement on pouvait ré-identifier un certain nombre de données de santé anonymes, par recoupement ou interconnexion de bases de données. D'où l'intérêt d'avoir des garde-fous pour éviter que la reconstitution de ces éléments soit aisée. Les personnes qui traitent des données sensibles doivent mettre en place des systèmes de sécurité pour les protéger vis-à-vis des tiers. On note de plus en plus de cas de hacking, soit pour récupérer des numéros de cartes bancaires, des identifiants bancaires, mais demain ce sera des dossiers complets de patients.

« On voit des éditeurs d'application de quantified self se positionner sur le marché du bien-être, »

Voilà pourquoi en France, contrairement à l'Europe, on a imposé un hébergeur agréé pour les données de santé. On a pris conscience que l'information de santé, doit être conservée auprès d'un hébergeur agréé par le ministère de la Santé, via l'Asip, pour garantir et certifier que la donnée est en lieu sûr. L'hébergeur est seulement dépositaire de cette information qu'il n'a pas le droit d'exploiter ni de communiquer à des tiers. C'est un coffre-fort. Il s'agit d'éviter une utilisation non appropriée de ce genre d'informations sensibles.

Un jour les assureurs pourront-ils avoir accès à ces données biologiques ou physiologiques sur la personne afin de moduler leur offre contractuelle ?
Cela commence déjà. Au printemps 2014, un partenariat a été mené entre Withings et Axa qui consistait à proposer la remise d'un podomètre à tout souscripteur d'une complémentaire santé Axa. L'information relative au nombre de pas faits par une personne n'était pas envoyée à Axa directement mais à Withings qui enregistrait l'information. Parallèlement, un jeu concours était organisé qui reposait sur la remise de bons cadeaux à qui faisait un nombre de pas minimum par jour. Les souscripteurs Axa pouvait gagner ces bons cadeaux. Axa n'avait certes pas l'information précise mais il savait clairement que les personnes à qui allaient être remis ces cadeaux avaient rempli le contrat du nombre de pas. L'assureur avait donc l'information sur les « bons » assurés. Il me semble que c'est un premier pas. Par ailleurs, Axa a monté un fond pour soutenir les projets en lien avec les objets connectés. S'il s'intéresse à ce sujet, c'est qu'il y voit son intérêt.

Et juridiquement, est-ce qu'un assureur peut se servir de cette information ?
Pour l'instant non, car cela reste une donnée sensible. Quand on travaille avec des assureurs, on le fait par l'intermédiaire d'un médecin ou un laboratoire mandé par l'assureur qui va communiquer quelques informations à ce dernier. En revanche, l'analyse des risques est faite par le médecin, l'assureur n'aura pas l'information de base. N'oublions pas le respect du secret médical.

Le projet de loi sur la santé prévoit l'ouverture des données de santé publique. Cela peut rendre de grands services, mais n'ouvre-t-on pas la boîte de Pandore car on sait aujourd'hui que les données anonymisées peuvent être repersonnalisées ?
Pour moi, on n'ouvre pas du tout la boîte de Pandore. Je suis en fait déçu par ce texte car l'ouverture des données est limitée à un nombre restreint de personnes. Dans l'étude d'impact qui accompagne le projet de loi, il est envisagé qu'un certain nombre d'opérateurs dont les laboratoires pharmaceutiques puissent mener leurs propres études pour comprendre le fonctionnement de leurs produits. Il y est affirmé que cette ouverture est une opportunité pour la France car cela va attirer des entreprises étrangères. Mais ce n'est pas ce qui ressort du texte. Car ne pourront utiliser ces données que ceux qui ont un projet d'intérêt général. Or, celui qui veut mieux comprendre ou améliorer le fonctionnement de son médicament ne poursuit pas, à mon sens, un projet d'intérêt général.

N'est-ce pas quand même de la santé publique ?
L'intérêt général n'est pas défini. Cela concerne plutôt le système de santé, la prise en charge des soins, etc. Si le texte reste en l'état, l'utilisation restera encore très restrictive avec de lourdes procédures pour obtenir des données dé-identifiées et travailler dessus.
Il faut une ouverture contrôlée de ces données dé-identifiées pour garantir le respect du secret médical et la vie privée des personnes. On doit vraiment pouvoir utiliser largement ces données pour améliorer de manière conséquente les connaissances scientifiques, celles sur les prises en charge des pathologies, les connaissances médico-économiques, dans l'objectif d'optimiser la prise en charge des patients français.

Quel impact ces technologies connectées va avoir sur notre manière d'envisager la santé ?
Ces technologies vont modifier en profondeur les relations patient/médecin. Elles concourent à un mouvement de fond qu'est la médecine personnalisée. Nous avons désormais des outils qui permettent d'avoir des informations très précises pour cibler des thérapeutiques. Parallèlement avec l'exploitation des big data, on arrive à affiner le diagnostic et les prescriptions car la personne a un profil génétique ou médical qui est identifié

Propos recueillis par Sylvie ROZENFELD