Les Cahiers de droit de la santé, numéro sous la direction de Guylène Nicolas et Vincent Vioujas intitulé « La modernisation du système de santé : un an d'application de la loi du 26 janvier 2016 », 2017, n°24, pp. 211-226.

Le rapport du patient à ses données à caractère personnel dans la loi de modernisation de notre système de santé : une mutation en marche

Sophie Gambardella
Docteur en droit, Aix Marseille Université, Université de Toulon, Univ Pau & Pays Adour, CNRS, DICE, CERIC, Aix-en-Provence, France.

Introduction

Depuis son adoption, la loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé a déjà fait couler beaucoup d'encre[1]. Le projet de loi, déposé à l'Assemblée nationale le 15 octobre 2014, entendait relever les nouveaux défis auxquels notre système de santé est aujourd'hui confronté notamment le vieillissement de la population, l'augmentation des maladies chroniques ou encore l'innovation en matière de santé. Pour y parvenir, il n'aura fallu pas moins de 227 articles qui attestent de la complexité d'une loi qui entend réformer en profondeur l'ensemble de notre système de santé. L'ampleur de l'ambition annoncée laisse alors craindre un manque d'aboutissement des dispositifs mis en place tant la tâche est lourde et sa mise en œuvre n'en sera pas moins.

Au sein de cette étude, le focus est fait sur l'un des aspects les plus sensibles de la loi de modernisation de notre système de santé : la protection des données à caractère personnel. Le développement du numérique dans le domaine de la santé a augmenté de manière exponentielle le traitement de données à caractère personnel. Les données à caractère personnel englobe « toute information concernant une personne physique identifiée ou identifiable (personne concernée) » de manière directe ou indirecte[2]. Les données à caractère personnel bénéficient alors normalement d'une protection juridique en ce qui concerne leur collecte, leur traitement et leur échange afin de permettre le respect de la vie privée. Par ailleurs, au sein de la catégorie des données à caractère personnel, une sous-catégorie de données dîtes « particulières » ou « sensibles », dont la protection doit être renforcée, a été identifiée. Parmi ces données sensibles se trouvent les données de santé. Avant l'adoption du nouveau règlement européen général sur la protection des données à caractère personnel, aucun texte juridique ne définissait la notion de données de santé. Dorénavant est considérée comme une donnée de santé « les données à caractère personnel relatives à la santé physique ou mentale d'une personne physique, y compris la prestation de services de soins de santé, qui

[1] Loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé, *J.O.R.F.* n°0022 du 27 janvier 2016, texte n° 1, NOR: AFSX1418355L. Pour des écrits sur la loi voir par exemple : Dossier spécial « Loi de santé », *RDSS*, n° 4, juillet-août 2016, pp. 597-708. ; ROMANENS (Jean-Louis), « Loi de modernisation de notre système de santé : le premier pas », *Revue Droit et santé*, n° 70, mars 2016, pp. 281-286. ; ROMANENS (Jean-Louis), « Loi de modernisation de notre système de santé : Chronique d'une naissance dénoncée », *Revue Droit et santé*, n° 69, janvier 2016, pp. 22-33. ; SIDEL (Juliette), TABUTEAU (Didier), BIZARD (Frédéric), « Loi santé : un ambitieux fourre-tout – Dossier », *Gazette santé social*, n° 125, janvier 2016, pp. 15-21. ; GIBELIN (Jean-Luc), « Loi santé : un déni de démocratie, un recul du service public, une régression sociale ! », *Cahiers de santé publique et de protection sociale*, n° 19, décembre 2015, pp. 30-34. ; LOMBRAIL (Pierre), « La loi de santé est votée : loi de santé ? », *Santé Publique*, vol.27, n° 6, novembre-décembre 2015, pp. 781-783. Pour un commentaire complet de la loi voir : CLEMENT (Jean-Marie), *La loi santé 2016 : Analyse, commentaires, critiques*, Bordeaux, Les Etudes Hospitalières (LEH), 2016, 158 p.

[2] Selon le Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 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 95/46/CE « est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale ».

révèlent des informations sur l'état de santé de cette personne »[3]. Cette définition fait ainsi entrer dans la catégorie des données dites « sensibles », toutes les données relatives aux interactions entre un patient et le système de santé. L'impératif de protection de l'ensemble de ces données a ainsi sous-tendu la rédaction de la loi du 26 janvier 2016. Toutefois, dans le domaine de la santé, la protection des données à caractère personnel est une question qui reste épineuse car elle met en tension l'intérêt collectif et l'intérêt personnel. Dans l'intérêt collectif, le partage et l'accès aux données produites dans le domaine de la santé devraient être renforcés pour non seulement améliorer la vigilance sanitaire mais aussi la qualité des soins en coordonnant davantage le parcours de santé du patient. Dans l'intérêt personnel, il conviendrait, en revanche, pour assurer aux mieux la protection de la vie privée de chacun de limiter le partage et l'accès aux données produites dans le domaine de la santé dans la mesure où une grande partie de ces données sont des données à caractère personnel. Si la modernisation de notre système de santé nécessitait de réfléchir sur l'opportunité d'augmenter le partage et l'accès aux données, toute la difficulté résidait dans la recherche du juste équilibre entre objectifs divergents.

Afin de mesurer l'équilibre trouvé au sein de la loi de modernisation de notre système de santé entre intérêt collectif et intérêt personnel, la réflexion sera menée selon deux axes. Un premier axe de recherche invitera à analyser les modifications apportées par la loi quant au partage des données à caractère personnel. Le règlement européen de 2016 et loi française du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés[4] affirment le principe d'interdiction de traitement des données de santé. Toutefois, des exceptions à ce principe sont prévues et les traitements des données de santé sont notamment licites s'il sont « nécessaires aux fins de la médecine préventive, des diagnostics médicaux, de l'administration de soins ou de traitements, ou de la gestion de services de santé et mis en œuvre par un membre d'une profession de santé, ou par une autre personne à laquelle s'impose en raison de ses fonctions l'obligation de secret professionnel ». Le secret professionnel est ainsi la clé de voûte de la protection des données de santé lorsque celles-ci font l'objet d'un traitement dans le cadre du parcours de santé. Dans un contexte où le partage des données produites dans le cadre du parcours de santé est de plus e plus large, le secret professionnel peut-il néanmoins encore assurer son rôle de garant de la vie privée ? (I.) Le second axe de recherche traitera de l'ouverture d'accès aux données générées dans le parcours de santé. Le secret professionnel ne peut ici plus être le garant de la protection des données personnelles dans la mesure où les données échappent aux professionnels de santé. Ce nouvel environnement nécessite, dès lors, que la sécurité des données soit assurée par d'autres outils dont l'efficacité peut être remise en cause (II).

I – Moderniser notre système de santé par l'extension du partage des données personnelles : une reconfiguration de la relation patient/médecin.

Dans le cadre de la relation patient-médecin, les données échangées sont placées sous le sceau du secret professionnel. Le personnel médical est, en effet, lié par le serment d'Hippocrate qu'il a prononcé et notamment par ces termes : « Admis(e) dans l'intimité des personnes, je tairai les secrets qui me seront confiés. Reçu(e) à l'intérieur des maisons, je respecterai les secrets des foyers et ma conduite ne servira pas à corrompre les mœurs ». Pourtant depuis la concrétisation de la dématérialisation du dossier médical par la mise en

[3] Article 4 -15) du Règlement (UE) 2016/679 du 27 avril 2016.
[4] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

place du dossier médical personnel (DMP)[5], le secret médical apparaît comme un secret partagé en dehors de la stricte relation patient-médecin. Or, la loi du 26 janvier 2016 accroît ce sentiment tant le patient semble être « déconnecté » de ses données (A.). Des efforts sont, en revanche, faits pour renforcer la sécurité des données de santé numérique. Toutefois, le développement croissant du numérique en vue d'améliorer les relations entre soignants et donc la coordination du parcours de soins ne se fait-il pas au détriment de la qualité des relations entre soignants et soignés ? (B.).

A. L'affaiblissement des droits du patient sur ses données de santé

Créé par la loi du 24 août 2004, le dossier médical personnel s'est vu remanié par la loi du 26 janvier 2016 sur la modernisation de notre système de santé. Il s'intitule dorénavant dossier médical partagé. Autrefois sous le giron de l'ASIP-Santé, la gestion du dossier médical partagé sera dorénavant assurée par la Caisse nationale d'assurance maladie des travailleurs salariés. Le changement de dénomination de ce dossier n'est pas anodin. Qualifier le dossier médical de « personnel » permettait de mettre l'accent sur le caractère particulier des données qu'il contient. Les données de santé sont, en effet, des données à caractère personnel dont la protection doit être renforcée en raison de leur caractère sensible. Pourtant la loi du 26 janvier 2016 en qualifiant le dossier médical non plus de « personnel » mais de « partagé » semble vouloir faire glisser le contrôle du traitement des données des mains du patient vers celles des professionnels de santé. A travers l'analyse du décret n° 2016-914 du 4 juillet 2016 relatif au dossier médical partagé[6], il conviendra, dès lors, de s'interroger sur la philosophie qui sous-tend la mise en place de ce nouveau dossier.

Le nouveau article L. 1111-14 du code de la santé publique prévoit qu'en ce qui concerne la création du dossier médical partagé, le patient reste au cœur du système dans la mesure où son consentement est nécessaire pour la mise en place de son dossier médical et où il en demeure le titulaire. De plus, le titulaire du dossier médical partagé à un droit d'accès à son dossier (article R. 1111-35 du code de la santé publique) ; de rectification de ses données (article R. 1111-37 du code de la santé publique) ; d'opposition à l'accès à ses données (article R. 1111-38 et R. 1111-39 du code de la santé publique) et enfin un droit de clôture de son dossier médical partagé (article R. 1111-34 du code de la santé publique). Toutefois, tous ces droits n'ont pas la même portée : certains semblent absolus alors que d'autres ont un exercice limité. Le titulaire du dossier médical possède le contrôle sur le partage de son dossier dans la mesure où il lui revient d'en autoriser ou non l'accès aux professionnels de santé. Toutefois, le titulaire du dossier médical partagé, en autorisant l'accès à son dossier à un professionnel de santé, autorise dans le même temps l'ensemble de l'équipe de soins[7] à accéder à son dossier. Le consentement est alors collectif et non

[5] Sur les étapes de mise en place du dossier médical personnel voir notamment : MONNIER (Anne), « Le Dossier Médical Personnel : histoire, encadrement juridique et perspectives », *RDSS*, n°4, 2009, pp. 625-634.

[6] Décret n° 2016-914 du 4 juillet 2016 relatif au dossier médical partagé, *J.O.R.F.* n°0155 du 5 juillet 2016, texte n° 20, NOR: AFSZ1609256D.

[7] La notion d'équipe de soins est définie à l'article L. 1110-12 du code de la santé publique de la manière suivante : « l'équipe de soins est un ensemble de professionnels qui participent directement au profit d'un même patient à la réalisation d'un acte diagnostique, thérapeutique, de compensation du handicap, de soulagement de la douleur ou de prévention de perte d'autonomie, ou aux actions nécessaires à la coordination de plusieurs de ces actes, et qui :

1° Soit exercent dans le même établissement de santé, au sein du service de santé des armées, dans le même établissement ou service social ou médico-social mentionné au I de l'article L. 312-1 du code de l'action sociale et des familles ou dans le cadre d'une structure de coopération, d'exercice partagé ou de coordination sanitaire ou médico-sociale figurant sur une liste fixée par décret ;

spécifique. L'article R. 1111-38 du code de la santé publique met, toutefois, un garde-fou à cette pratique du consentement collectif en permettant au titulaire du dossier d'interdire l'accès à son dossier à certains professionnels de santé autorisés à y accéder. Il reste que le principe demeure celui du consentement collectif et l'exception celui de l'exclusion d'un professionnel de santé. Le secret médical devient ainsi dans le même temps un secret collectif. Cette disposition se comprend dans un objectif d'amélioration de la coordination du parcours de santé du patient mais elle interroge tout de même sur le réel contrôle dont dispose le patient sur le partage de ses données d'autant plus que le médecin traitant a, quant à lui, un accès illimité au dossier médical de son patient. Le titulaire ne peut donc pas dissimuler certaines informations à son médecin traitant mais il ne peut, de plus, pas lui même, supprimer les données inscrites par un professionnel de santé dans son dossier. Il doit en faire la demande auprès du professionnel de santé et prouver l'existence d'un motif légitime justifiant une telle suppression. Le fait que ses données sensibles soient en ligne n'est-il pas, en soi, un motif légitime pour disposer du choix des données contenues dans le dossier médical partagé ? Il semble que non. Les objectifs de coordination et d'amélioration de la qualité des soins ont ainsi pris le pas sur l'intérêt personnel du patient. Il pourrait être avancé que le dispositif est mis en place avant tout dans l'intérêt du patient dans la mesure où il bénéficiera d'une prise en charge médicale de meilleure qualité. Toutefois, le patient perd, dans le même temps, une partie de son libre arbitre notamment le choix de ne pas savoir car une fois les données transmises à l'équipe de soins, il sera certainement, pour lui, plus difficile de refuser une prise en charge médicale. Même si les données contenues dans le dossier médical partagé sont couvertes par le secret médical, ce secret est dorénavant partagé ce qui implique pour le patient, certes une protection de sa vie privée, mais certainement un affaiblissement de sa liberté au sein de sa vie privée.

Avec la création d'un dossier médical partagé, le patient perd en quelque sorte la paternité de ses données alors même que l'environnement en ligne augmente les risques d'atteinte à sa vie privée. Cette crainte est d'autant moins théorique qu'en juin 2016, la presse révélait qu'aux Etats-Unis près de 655 000 enregistrements, contenant des informations sur des patients américains, ont été volés à plusieurs groupes d'assurance santé américains pour être revendus. En France, en 2015, le laboratoire Labio a lui aussi fait l'objet d'un piratage par Rex Mundi qui a divulgué les données médicales de 15 000 patients. Sur l'année 2015, ce ne sont pas moins de 1300 attaques informatiques contre des établissements de santé qui ont été signalées. Or, cette tendance continue de s'accroître car d'une part, les données de santé représentent une manne financière très importante et d'autre part, ces données sont faciles à voler car leur sécurité est bien souvent faillible. Dans ce contexte, la création de dossiers médicaux partagés laisse perplexe d'autant plus que même si le titulaire demande la clôture de son dossier celui-ci est conservé encore dix ans par la CNAMTS. Il paraissait alors nécessaire en parallèle de renforcer la sécurité des données médicales notamment en confortant les exigences de sécurité imposées aux hébergeurs de données de santé.

B. Le renforcement de la sécurité de l'hébergement des données de santé

La loi de modernisation de notre système de santé envisage une profonde refonte du régime juridique applicable aux hébergeurs de données de santé. L'objectif est de renforcer la sécurité des données de santé et donc, par ricochet, la protection de la vie privée des patients.

2° Soit se sont vu reconnaître la qualité de membre de l'équipe de soins par le patient qui s'adresse à eux pour la réalisation des consultations et des actes prescrits par un médecin auquel il a confié sa prise en charge ;
3° Soit exercent dans un ensemble, comprenant au moins un professionnel de santé, présentant une organisation formalisée et des pratiques conformes à un cahier des charges fixé par un arrêté du ministre chargé de la santé ».

L'article 204-I-5°-c) de la loi du 26 janvier 2016 remplace ainsi la procédure d'agrément par une procédure de certification. Une ordonnance en date du 12 janvier 2017, qui devra être précisée par un décret, met en place cette procédure[8]. Selon le nouvel article L. 1111-8 du code de la santé publique, la certification sera réalisée par un organisme accrédité par le comité français d'accréditation ou par l'instance nationale d'accréditation d'un autre Etat membre de l'Union européenne. L'objectif est alors de renforcer la sécurité des données en recourant notamment à la procédure de certification ISO 27001. De ce point de vue là, le nouveau dispositif, qui devra être précisé, redonne aux données de santé leur place de données à caractère sensible devant faire l'objet d'une protection renforcée. Toutefois, un élément de la réforme engagée par la loi du 26 janvier 2016 interroge de nouveau sur le lien entre le patient et ses données de santé.

Le nouvel article L. 111-8 du code de la santé publique remplace le consentement explicite du patient à l'hébergement externalisé de ses données par une simple obligation d'information de celui-ci. Le patient peut, par ailleurs, s'opposer à l'hébergement de ces données à condition qu'un motif légitime le justifie. Cette disposition de l'article fait largement écho à la modification apportée par la loi du 26 janvier 2016, quant à la demande de suppression par le patient de certaines données inscrites dans son dossier médical partagé. Là encore, le consentement du patient n'est plus la condition de licéité du traitement de ses données de santé. L'article 8-II 6°) de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés prévoit une autre condition de licéité du traitement des données de santé. En effet, le traitement est licite s'il est « nécessaire aux fins de la médecine préventive, des diagnostics médicaux, de l'administration de soins ou de traitements, ou de la gestion de services de santé et mis en œuvre par un membre d'une profession de santé, ou par une autre personne à laquelle s'impose en raison de ses fonctions l'obligation de secret professionnel ». Ce n'est donc pas la licéité du traitement des données du patient qui est ici en cause mais davantage la philosophie qui sous-tend ce mouvement de contournement du consentement du patient. En écartant le consentement du patient des procédures de traitement de ses données, le législateur semble refuser d'opérer une subjectivisation du droit. Le patient n'est pas considéré comme propriétaire de l'« objet » ou des « faits » appelés données de santé. La loi du 26 janvier 2016 marque ainsi clairement le refus de la France de s'insérer dans une philosophie de patrimonialisation des données[9]. La protection de la vie privée du patient ne peut alors être incarnée par un droit de propriété de ce dernier sur ses données. Le secret médical reste la clé de voûte de cette protection. De plus, l'expression « motifs légitimes » laisse transparaître un jugement de valeur porté, *a priori* par le professionnel de santé, sur les motifs qui sous-tendent la demande du patient. La relation patient-médecin est ainsi transformée non seulement par le partage du secret médical mais aussi parce que le professionnel de santé va devoir évaluer les demandes émises par le patient. La relation de confiance entre le patient et le professionnel de santé risque d'en souffrir alors même que le contexte anxiogène du numérique devrait conduire au contraire à rechercher à renforcer cette relation.

La loi de modernisation de notre système de santé a donc œuvré pour un renforcement de la sécurité des données hébergées et, dans le même temps, a cherché à renforcer le « tout numérique ». L'article 204-I 5°) d) de la loi entendait mettre fin à la conservation des dossiers

[8] Ordonnance n° 2017-27 du 12 janvier 2017 relative à l'hébergement des données de santé à caractère personnel, *J.O.R.F.* du 13 janvier 2017, texte 17, NOR : AFSZ1626575R.

[9] Sur le numérique et la patrimonialisation des données voir notamment : LACOUR, (Stéphanie), « Nouvelles technologies et patrimonialisation des données personnelles : un changement de paradigme ? », *in* VIOLET (Franck), *Personne et patrimoine en droit*, Bruxelles, Bruylant, 2015, pp. 363-384.

médicaux papiers à condition que leur copie numérique ait force probante. Le 5 décembre 2016, le décret n° 2016-1673 du 5 décembre 2016 relatif à la fiabilité des copies pris pour l'application de l'article 1379 du code civil reconnaissait la force probante, à certaines conditions, des copies numériques de documents[10]. Ce décret a alors été suivi, le 12 janvier 2017, de l'ordonnance n°2017-29 qui a détaillé les conditions de reconnaissance de la force probante des documents comportant des données de santé à caractère personnel créés ou reproduits sous forme numérique et de destruction des documents conservés sous une autre forme que numérique[11]. Dorénavant la copie numérique d'un document produit dans le cadre du parcours de soin du patient aura la même force probante que le document papier original. Selon l'article 1379 du code civil, en cas de doute sur la fiabilité du document, la charge de la preuve incombera à celui qui conteste son authenticité. De plus, les professionnels, services, établissements ou organismes de santé pourront produire à la demande des personnes intéressées des documents numériques à partir de données contenues dans plusieurs autres documents. Là encore, le patient sera simplement informé de l'informatisation de ses données de santé et de la valeur des documents numériques ainsi produits mais son consentement n'est en aucun cas requis. La relation duale patient-médecin est ainsi reconfigurée et devient une relation avec une interface numérique omniprésente. Dans ce nouveau contexte, le secret médical même partagé demeure le dernier rempart fiable face aux atteintes à la vie privée car, lorsque les données sont partagées en dehors du sceau du secret médical, leur sécurité devient très faillible.

II – Moderniser le système de santé par l'ouverture de l'accès aux données : une brèche dans la sécurité des données personnelles.

L'ouverture de l'accès aux données de santé par la loi du 26 janvier 2016[12], au travers de l'article 193, s'inscrit dans un mouvement, en France, de renforcement des exigences de démocratie et de transparence venant renouveler les relations entre l'administration et le public[13]. Toutefois, l'ouverture de l'accès aux données dans le domaine de la santé présente des risques d'atteinte à la vie privée dans la mesure où les données générées sont en grande partie des données à caractère personnel. L'*open data* en matière de santé, mis en place par la loi du 26 janvier 2016, doit alors faire l'objet d'un double questionnement : celui du « quoi » et celui du « qui ». Le premier questionnement invite à réfléchir sur la nature des données auquel l'accès devient ouvert (A.) alors que le second questionnement interroge sur les entités pouvant bénéficier de cet accès ouvert aux données (B.). Le regard porté sur ces deux aspects des modifications, apportées par la loi de modernisation de notre système de santé, à l'accès aux données de santé engagera plus globalement une réflexion sur la manière dont la vie privée est protégée dans un contexte d'*open data*.

A. La sécurité fragile des données ouvertes en matière de santé

[10] Décret n° 2016-1673 du 5 décembre 2016 relatif à la fiabilité des copies et pris pour l'application de l'article 1379 du code civil, NOR: JUSC1624640D.

[11] Ordonnance n°2017-29 du 12 janvier 2017 relative aux conditions de reconnaissance de la force probante des documents comportant des données de santé à caractère personnel créées ou reproduits sous forme numérique et de destruction des documents conservés sous une autre forme que numérique, *J.O.R.F.* du 12 janvier 2017, texte 21, NOR : AFSZ1630603R.

[12] Pour une autre étude sur le sujet voir : CATTAN (Jean), « La mise à disposition des données de santé », *Droit administratif*, n°5, mai 2016, étude n° 9, p. 15.

[13] Sur la politique française d'ouverture de l'accès aux données publiques voir notamment VERDIER (Henri) et VERGNOLLE (Suzanne), « L'Etat et la politique d'ouverture en France », *A.J.D.A.*, n°2, 25 janvier 2016, pp. 92-96.

Le chapitre V de la loi de modernisation de notre système de santé, intitulé « créer les conditions d'un accès ouvert aux données de santé », complète le livre IV du code de la santé publique par un titre VI « Mise à disposition des données de santé » et met en place pour la réalisation de cet *open data* en matière de santé, le système national des données de santé (SNDS). Ce système a pour ambition de rassembler plusieurs bases de données, exhaustivement listées, qui seront mises à disposition du public. Le système doit, par ailleurs, traiter les données de manière à assurer une protection de la vie privée des personnes concernées. A cette fin, les données individuelles du SNDS ne peuvent, par exemple, être conservées que pour une durée maximale de vingt ans. L'article L. 1461-1 du code de la santé publique, créé par la loi du 26 janvier 2016, énumère les cinq bases de données qui nourriront le SNDS[14]. La base de données ainsi constituée sera très large, comme en atteste le décret n° 2016-1871 du 26 décembre 2016 relatif au traitement de données à caractère personnel dénommé « système national des données de santé »[15]. Ce décret vient préciser les modalités de mise en œuvre du SNDS en ajoutant un article R. 1461-4 au code de la santé publique et détaille les catégories de données réunies au sein du SNDS[16].

Le SNDS contiendra notamment « les informations relatives aux bénéficiaires de soins et de prestations médico-sociales ». Cette catégorie de données est la plus sensible dans une perspective de protection de la vie privée des personnes concernées en contexte d'*open data*. Les données rendues accessibles ne doivent, en effet, pas être nominatives pour répondre à l'exigence de protection de la vie privée. Dès lors, le décret précise que, si cette catégorie de données inclut le sexe, le mois, l'année de naissance, le rang de naissance, le lieu de résidence, les informations médico-administratives et le cas échéant, les informations relatives au décès, elle ne doit, en revanche, pas faire mention ni du nom, ni du prénom ou encore de l'adresse du bénéficiaires de soins et de prestations médico-sociales[17]. Le caractère non

[14] Le système contiendra ainsi les données produites dans le cadre du Programme de médicalisation des systèmes d'information (PMSI) ; les données du Système national d'information inter-régimes de l'assurance maladie (SNIIRAM) ; les données sur les causes de décès mentionnées à l'article L. 2223-42 du code général des collectivités territoriales ; les données médico-sociales produites par les maisons départementales des personnes handicapées ; ainsi qu'un échantillon représentatif des données de remboursement par bénéficiaire transmises par des organismes d'assurance maladie complémentaire et défini en concertation avec leurs représentants.

[15] Décret n° 2016-1871 du 26 décembre 2016 relatif au traitement de données à caractère personnel dénommé « système national des données de santé, *J.O.R.F.* n°0301 du 28 décembre 2016, texte n° 33, NOR : AFSE1625287D.

[16] Selon l'article R. 1461-4 du code de la santé publique, les catégories de données réunies au sein du système national des données de santé sont les suivantes :

1) Les informations relatives aux bénéficiaires de soins et de prestations médico-sociales ;

2) Les informations relatives aux organismes d'assurance maladie obligatoire et, s'il y a lieu, aux organismes d'assurance maladie complémentaire intervenant dans la prise en charge financière du bénéficiaire des soins et prestations ;

3) Les informations relatives à la prise en charge sanitaire, médico-sociale et financière associées à chaque bénéficiaire ;

4) Les informations relatives aux professionnels et services de santé intervenant dans la prise en charge des bénéficiaires mentionnés au I :

5) Les informations médico-sociales relatives à la situation des personnes en situation de handicap transmises à la Caisse nationale de solidarité pour l'autonomie dans le cadre du système d'information mentionné à l'article L. 247-2 du code de l'action sociale et des familles :

6) Les informations relatives aux arrêts de travail et aux prestations en espèces : les données relatives aux arrêts de travail, au versement d'indemnités journalières pour les risques maladie, maternité, paternité, accidents du travail et maladies professionnelles et au versement de pensions d'invalidité, de rentes consécutives à un accident du travail ou à une maladie professionnelle ou de capitaux décès.

[17] Article R. 1461-4 du code de la santé publique.

nominatif de ces données est alors assuré par un pseudonyme[18]. L'article R 1461-7 1°) du code de la santé publique précise que la procédure de pseudonymisation des données de santé doit être organisée « de sorte que nul ne puisse disposer à la fois de l'identité des personnes, notamment de leur numéro d'inscription au Répertoire national des personnes physiques, d'une part, et du pseudonyme […] d'autre part ». En théorie, la sécurité des données devrait être ainsi assurée par le fait qu'elles demeurent des données non nominatives. Toutefois, comme la ré-identification des données est possible, puisque coexistent d'un côté, le code et de l'autre, le numéro d'inscription au Répertoire national d'identification des personnes physiques, ces données demeurent des données à caractère personnel. En effet, le règlement européen de 2016 précise qu'« est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale ». Les risques d'atteinte à la vie privée en cas notamment de piratage du SNDS sont donc réels. De nombreux auteurs ont déjà mis en garde sur les risques d'atteinte au droit à la vie privée dans le cadre de l'*open data* en matière de santé[19] et sur l'impossibilité à travers l'utilisation exclusive de la technique de la pseudonymisation d'assurer une protection effective de la vie privée. Il faut, en effet, garder à l'esprit que « la pseudonymisation réduit [certes] le risque de mise en corrélation d'un ensemble de données avec l'identité originale d'une personne concernée ; à ce titre, c'est une mesure de sécurité utile, mais non une méthode d'anonymisation »[20]. De plus, même l'anonymisation des données ne certifie pas que l'identification des personnes concernées soit impossible dans la mesure où certaines données semblent intrinsèquement identifiante. A titre d'exemple, face à une maladie très rare, le nombre de patients à l'échelle mondiale est réduit et le risque d'identification d'un d'entre eux existe malgré la mise en œuvre d'une méthode d'anonymisation des données. Les risques d'atteinte à la vie privée sont donc réels dès lors qu'est mis en place l'*open data* d'autant plus qu'en matière de santé les données générées sont pour certaines des données dites sensibles notamment celles qui portent sur l'état pathologique de la personne concernée. Ce risque d'atteinte à la vie privée est, par ailleurs, renforcé au sein du SNDS par deux facteurs identifiés par la Commission nationale de l'informatique et des libertés (CNIL), dans son avis sur le décret n° 2016-1871 du 26 décembre 2016[21].

La CNIL s'était, en premier lieu, déjà inquiétée des risques de ré-identification des personnes notamment en raison de la mise à disposition de divers échantillons de données. L'article R. 1461-5 prévoit, en effet, que puissent être constitués à partir du SNDS des jeux de données anonymes à destination du public ; des jeux de données agrégées et semi-agrégées adaptés à différents types de recherches, d'études ou d'évaluation ; des échantillons généralistes représentatifs de l'ensemble des bénéficiaires de l'assurance maladie. La

[18] Selon l'article R. 1461-4 du code de la santé publique, le pseudonyme est « constitué d'un code non signifiant obtenu par un procédé cryptographique irréversible du numéro d'inscription au Répertoire national d'identification des personnes physiques ».

[19] Voir par exemple : CASTETS-RENARD (Céline), « Les opportunités et risques pour les utilisateurs dans l'ouverture des données de santé : big data et open data », *Revue Le Lamy Droit de l'immatériel*, n°108, octobre 2014, pp. 38-45. ; CLUZEL-METAYER (Lucie), « Les limites de l'*open data* », AJDA, n°2, 2016, p. 102-107.

[20] Groupe de travail « article 29 » sur la protection des données 0829/14/FR WP216 Avis 05/2014 sur les Techniques d'anonymisation, adopté le 10 avril 2014. Ce groupe de travail a été institué par l'article 29 de la directive 95/46/CE. Il s'agit d un organe consultatif européen indépendant sur la protection des données et de la vie privée.

[21] Commission nationale de l'informatique et des libertés, délibération n° 2016-316 du 13 octobre 2016 portant avis sur un projet de décret en Conseil d'Etat relatif au Système national des données de santé (demande d'avis n° 16018114), *J.O.R.F.* du 28 décembre 2016, texte n° 189, NOR : CNIX1638410X.

multiplication des jeux de données peut alors être la clé pour une ré-identification par croisement des informations de celles-ci. Le risque dans cette situation ne provient plus réellement de la procédure de pseudonymisation mais davantage du risque que des tiers détenant d'autres informations sur une personne puissent par croisement des données parvenir à la ré-identifier. Il s'agit donc là d'un second niveau de risque pour le droit à la vie privée dans la mesure où l'intention d'un tiers procédant de la sorte peut difficilement être appréhendée comme dénué d'intérêt financier. La CNIL avait préconisé qu'une analyse des risques soit faite avant la constitution de chaque échantillon de données ou de chaque jeu de données. Si une telle recommandation ne trouve pas écho dans le texte du décret n° 2016-1871 du 26 décembre 2016, il est *a priori* possible de minimiser en partie le risque de ré-identification des données par des tiers. L'article L. 1461-2 du code de la santé publique, mis en place par la loi du 26 janvier 2016, précise que les données qui sont mises gratuitement à disposition du public sont uniquement celles qui prennent la forme « de statistiques agrégées ou de données individuelles constituées de telle sorte que l'identification directe ou indirecte, des personnes concernées y est impossible ». De plus l'utilisation de ces données ne peut avoir ni pour objet ni pour effet d'identifier les personnes. Le risque de ré-identification est donc normalement maîtrisé puisque les autres jeux de données devront faire l'objet d'une demande. Toutefois, la seconde inquiétude de la CNIL relativise nettement cette affirmation dans la mesure où cette dernière estime que « le procédé cryptographique utilisé au lancement du SNDS sera celui du SNIIRAM, procédé dont la robustesse est aujourd'hui remise en question par l'ancienneté de son algorithme et par le fait que les secrets cryptographiques n'ont jamais été renouvelés ». Cette faiblesse dans la sécurité du SDNS avait déjà été relevée par la Cour des comptes en mai 2016[22] et interroge sur la fiabilité du système mis en place. Les exigences liées à la sécurité des données contenues dans le SDNS dans une perspective de respect de la vie privée ne semblent pas entièrement satisfaisantes à l'aune du lancement du SDNS – l'exigence de sécurité vis à vis de la CNAMTS étant, par exemple, inférieur à celui d'un hébergeurs de données de santé. Le renforcement de la sécurité des données du SNDS devrait d'autant plus être une priorité que le nombre d'acteurs qui vont pouvoir à l'avenir y accéder va se multiplier.

B. L'accès simplifié aux données dans le cadre de l'open data en matière de santé

Les doutes sur la sécurité des données contenues dans le SNDS sont amplifiés par la multiplication des acteurs pouvant y avoir accès. La loi du 26 janvier 2016 distingue trois types d'acteurs : les acteurs ayant un accès permanent à la base du SDNS, le public et les acteurs ayant accès au SNDS à des fins de recherche, d'études ou d'évaluations. Pour chacune de ces catégories, le degré d'ouverture de l'accès à la base de données du SNDS diffère.

L'article L. 1461-2 du code de la santé publique prévoit, en premier lieu, que les données ouvertes gratuitement au public sont celles dont l'identification directe ou indirecte de la personne concernée est rendue impossible ou encore celles prenant la forme de statistiques agrégées. Sont ainsi constitués, à cette fin, à partir du SNDS, des jeux de données anonymes. Il n'est pas nécessaire de revenir ici sur les réserves émises quant à la sécurité liée à ce type de données. En revanche, il convient de s'attarder sur le terme de « public » qui a pu susciter des interrogations quant à sa portée. Il semble que « les start-up, sans être désignés

[22] Cour des comptes, « Les données personnelles de santé gérées par l'assurance maladie : Une utilisation à développer, une sécurité à renforcer », *Communication à la commission des affaires sociales et à la mission d'évaluation et de contrôle des lois de financement de la sécurité sociale de l'Assemblée nationale*, Mars 2016. Disponible à l'adresse suivante : https://www.ccomptes.fr/Accueil/Publications/Publications/Les-donnees-personnelles-de-sante-gerees-par-l-assurance-maladie

spécifiquement au sein du « public », sont bien visées par la réutilisation de ces données anonymisées »[23]. Si cette porte ouverte sur les données en matière de santé au secteur privé est avant tout vue, notamment par la ministre Marisol Touraine, comme une opportunité en termes d'amélioration des soins, de vigilance sanitaire mais aussi de réduction des coûts, elle peut aussi être source d'inquiétude dans la mesure où elle permet notamment aux assurances ou encore aux établissements bancaires de recueillir des données sensibles[24]. La loi du 26 janvier 2016 pose néanmoins des gardes fous à cette réutilisation par le public de jeu de données issus du SNDS en excluant certaines finalités. Les données ainsi collectées ne peuvent, tout d'abord, pas servir à la promotion de produits sanitaires ou cosmétiques. L'exclusion de cette première finalité permet d'éviter que l'industrie pharmaceutique et l'industrie cosmétique n'utilisent ces données comme argument de vente de leurs produits. Ensuite, ces données ne peuvent être source d'exclusion de garanties des contrats d'assurance, de modification des cotisations ou encore de prime d'assurance. Si cette disposition est intéressante en ce qu'elle permet d'exclure l'utilisation lucrative des données du SNDS par les compagnies d'assurance, elle ne couvre néanmoins pas toutes les hypothèses. Ainsi, les établissements bancaires peuvent, par exemple, avoir intérêt à obtenir ce type de données pour refuser un prêt à une personne malade ou pour augmenter l'assurance de ce prêt. L'*open data* fait ainsi peser un risque non négligeable sur le droit au respect de la vie privée dans la mesure où malgré les précautions prises en amont pour assurer la sécurité des données, le système ne peut en aucun cas être infaillible.

En deuxième lieu, un accès aux données à caractère personnel du SNDS peut être autorisé au cas par cas à des fins de recherche, d'étude ou d'évaluation permettant d'améliorer la qualité des soins, la vigilance sanitaire ou encore de réduire les dépenses de santé. Le décret n° 2016-1872 du 26 décembre 2016 est venu préciser les modalités de demande d'autorisation d'accès au SNDS dans ce cadre[25]. La lecture de ce décret met en exergue la volonté de simplifier l'accès aux données du SNDS à des fins de recherche, d'étude ou d'évaluations. En effet, deux procédures de demande d'autorisation sont prévues : l'une dite « standard » et la seconde simplifiée. Afin de mettre en œuvre la procédure dite « standard », une demande d'autorisation d'accès au SNDS doit être déposée auprès de l'Institut national des données de santé qui les transmet au Comité compétent – le Comité d'expertise pour les recherches, les études et les évaluations dans le domaine de la santé – pour avis. La décision d'autorisation d'accès au SNDS est prise en dernier ressort par la CNIL. En parallèle, une procédure simplifiée est mise en place pour les catégories les plus usuelles de traitement automatisé de données à caractère personnel. Dans cette hypothèse, la CNIL peut mettre en place des méthodologies de références. Or, si un responsable de traitement de données s'engage à respecter une des méthodologies, la CNIL peut délivrer une autorisation d'accès à certains jeux de données et échantillons mis à disposition par l'Institut national des données de santé sans que d'autres formalités soient requises. La procédure simplifiée permet sans conteste d'accroître les possibilités de traitement et d'utilisation des données du SDNS dans le cadre de recherche, d'étude et d'évaluation et répond par conséquent aux attentes en termes de vigilance sanitaire existantes depuis notamment le scandale du Médiator ou encore celui de la pilule « Diane 35 ». Cependant, l'ouverture de l'accès aux données aux fins de recherche,

[23] DEBIES (Elise), « L'ouverture et la réutilisation des données de santé : panorama et enjeux », *RDSS*, n°4, 2016, p. 698.

[24] Sur les pratiques des compagnies d'assurance voir notamment : LECU (Anne), *Le secret médical. Vie et mort*, Paris, Les Editions du Cerf, coll. Essais, 2016, note de bas de page 88.

[25] Décret n° 2016-1872 du 26 décembre 2016 modifiant le décret n° 2005-1309 du 20 octobre 2005 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, *J.O.R.F.* n°0301 du 28 décembre 2016, texte n° 34, NOR: AFSE1625288D

d'études ou d'évaluations peut être restreint par les droits des personnes concernées sur leurs données. En effet, la recherche de conciliation entre transparence et sécurité nécessitait de permettre aux personnes concernées non seulement d'être informée de l'accès à leurs données personnelles mais aussi de pouvoir faire valoir leurs droits d'accès, de rectification et d'opposition. Ainsi, la personne concernée peut s'opposer à ce que ses données fassent l'objet d'une levée du secret médical. Il reste donc un espace dans lequel, malgré le fort mouvement d'ouverture d'accès aux données, le secret médical dans sa conception la plus stricte reprend droit de séance.

En troisième lieu, certains acteurs peuvent obtenir un accès permanent à la base de données du SNDS comme le précise le décret n° 2016-1871 du 26 décembre 2016. L'article R. 1461-12 du code de la santé publique liste, de manière exhaustive, les services de l'Etat, les établissements publics et les organismes chargés d'une mission public autorisés à avoir un cet accès permanent à la base du SNDS[26]. L'autorisation permanente d'accès est toutefois encadrée par le décret n°2016-1871 du 26 décembre 2016. L'étendue de celle-ci est fonction de la « profondeur historique des données utilisées, l'aire géographique ou les caractéristiques d'une population déterminée au regard des finalités sanitaires ou sociales du traitement »[27] et du risque, dans la manière dont le traitement est effectué, d'accroître les possibilités de ré-identification. A partir de ces deux critères, des limites ont été posées pour chaque organisme quant aux données auxquelles l'accès leur été ouvert de manière permanente. Le décret de décembre 2016 a ainsi établi six niveaux d'accès permanent aux données du SNDS[28]. Par ailleurs, la profondeur historique maximale de traitement des données auquel chaque organisme a accès est là aussi différente pour chacun allant de 20 ans pour l'accès permanent le plus large à 6 ans pour l'accès permanent le plus restreint[29]. Or, si un organisme doit traiter des données ne s'inscrivant pas dans les limites posées à son autorisation d'accès permanent, une demande d'autorisation d'accès ponctuel à ces données devra être effectué, comme pour les traitements à des fins de recherche, d'études ou d'évaluations. Il est, toutefois, important de noter que si ce service obtient une autorisation ponctuelle d'accéder à des données du SDNS se situant en dehors de son périmètre d'autorisation permanente, la personne concernée ne pourra pas s'opposer au traitement de ses données. Le secret médical redevient alors un secret partagé avec les services de l'Etat et non simplement un secret dans la relation patient-

[26] « Les services de l'Etat, les établissements publics et les organismes chargés d'une mission de service public autorisés à traiter des données à caractère personnel du système national des données de santé en application du III de l'article L. 1461-3 sont les suivants : 1° La direction de la recherche, des études, de l'évaluation et des statistiques, la direction générale de la santé et la direction générale de l'offre de soins, la direction de la sécurité sociale, la direction du budget et le service de santé des armées ; 2° Les agences régionales de santé ; 3° Les caisses nationales des régimes de l'assurance maladie obligatoire, les organismes locaux et régionaux de l'assurance maladie obligatoire ; 4° La Caisse nationale de solidarité pour l'autonomie ; 5° La Haute Autorité de santé ; 6° L'Autorité de sûreté nucléaire ; 7° L'Agence nationale de santé publique ; 8° L'Agence nationale de sécurité du médicament et des produits de santé ; 9° L'Agence de biomédecine ; 10° L'Institut de radioprotection et de sûreté nucléaire ; 11° L'Institut national du cancer ; 12° L'Etablissement français du sang ; 13° L'Agence technique de l'information sur l'hospitalisation ; 14° L'Agence nationale d'appui à la performance des établissements de santé et médico-sociaux ; 15° L'Institut national des données de santé ; 16° L'Institut de recherche et documentation en économie de la santé ; 17° L'Institut national d'études démographiques ; 18° L'Observatoire français des drogues et toxicomanies ; 19° Le Haut Conseil pour l'avenir de l'assurance maladie ; 20° Le Fonds de financement de la couverture maladie universelle ; 21° Les observatoires régionaux de la santé ; 22° Les unions régionales de professionnels de santé ; 23° Les équipes de recherche de l'Institut national de la santé et de la recherche médicale ; 24° Les équipes de recherche des centres hospitaliers universitaires et des centres de lutte contre le cancer ; 25° Les équipes de recherche et de formation de l'Ecole des hautes études en santé publique ».

[27] Article R. 1461-11 du code de la santé publique.

[28] Article R. 1461-14 du code de la santé publique.

[29] Article R. 1461-13 du code de la santé publique.

médecin. Même si l'accès permanent aux données du SNDS est très encadré et ciblé en fonctions des finalités des traitement à effectuer, il reste que « ce sont plus de deux mille utilisateurs potentiels qui auront accès au SNDS, voire jusqu'à trois mille en comptant l'intégralité des Unions régionales des professionnels de santé. Sur ce total, plus de cinq cent utilisateurs seront dans des organismes qui ne possèdent pas aujourd'hui d'accès direct aux données du SNIIRAM ou du PMSL »[30]. Face à ce constat et en prenant acte des failles de sécurité du SNDS, les atteintes au droit au respect de la vie privée risquent de s'accroître.

Schématiquement, l'accès au SNDS peut se faire selon quatre voies : deux sans demandes autorisation d'accès et deux au travers d'une demande d'autorisation d'accès. En effet, d'un côté le public se voit mettre à disposition certaines données et certains services publics ont un accès permanent mais encadré au SNDS. D'un autre côté, l'accès aux données du SNDS à des fins de recherche, d'étude et d'évaluation fait l'objet d'une procédure d'autorisation pouvant être simplifiée et l'accès aux données du SNDS par certains services publics en dehors de leur périmètre d'autorisation permanente doit faire l'objet aussi d'une autorisation. La loi de modernisation de notre système de santé a donc sans conteste ouvert l'accès aux données dans le domaine de la santé. Toutefois, cette ouverture fait l'objet d'un encadrement strict et s'apparente, dès lors, davantage à une semi-ouverture. Reste que même si cette ouverture de l'accès aux données est restreinte, l'entrebâillement de cette porte ouvre un chemin d'accès à des éléments essentiels de la vie privée.

*****

Aborder par le prisme de la protection des données à caractère personnel, la loi de modernisation de notre système de santé semble porter une idéologie forte : une volonté de renouvellement des pratiques dans le secteur de la santé. Le renouvellement des pratiques s'incarne, en premier lieu, dans la reconfiguration de la relation patient-médecin. La relation intimiste placée sous le sceau du secret médical se mue en une relation éclatée, plurielle dans laquelle le patient est en prise avec une équipe de soins afin d'améliorer son parcours de santé. Le renouvellement des pratiques s'impose, en deuxième lieu, aux professionnels de santé qui doivent non seulement abandonner l'encre et la plume au profit de l'outil numérique mais qui doivent, de surcroît, gérer les données à caractère personnel de leurs patients, en accédant ou non aux demandes de ces derniers. Le renouvellement des pratiques est, enfin, matérialisé par l'ouverture de l'accès aux données de santé. Malgré sa position de deuxième pays d'Europe le plus mature en matière d'*open data*, la France a toujours eu de nombreuses réticences à ouvrir l'accès aux données collectées dans le domaine de la santé tant ces données sont sensibles. Ce pas franchi par la loi de modernisation de notre système de santé est donc emblématique de cette volonté de modifier les pratiques pour les adapter aux nouveaux enjeux sociétaux. Reste à espérer que d'une part, en bouleversant simultanément l'ensemble des pratiques, la loi du 26 janvier 2016 n'a pas ébranlé les fondations même du système de santé, nécessaires pour assurer en douceur la transition vers de nouvelles pratiques, et que d'autre part, la juste mesure des risques a été prise pour ne pas se bruler les ailes dans l'*open data*.

[30] Commission nationale de l'informatique et des libertés, délibération n° 2016-316 du 13 octobre 2016 portant avis sur un projet de décret en Conseil d'Etat relatif au Système national des données de santé (demande d'avis n° 16018114), *J.O.R.F.* du 28 décembre 2016, texte n° 189, NOR : CNIX1638410X.