Master 2 Droit de la Santé

Parcours « Droit et éthique des professions et des institutions de santé »

Continuité entre protection juridique de la personne et protection juridique des données de santé

Par Sophie LAMOUR

Sous la direction de Madame Florence EON

Directrice juridique de l'Agence des Systèmes d'Information Partagés de santé

Membres du jury :

- Monsieur Benoît APPOLIS, Maître de conférences en droit public à la Faculté de droit de l'Université de Rennes 1
- Madame Florence EON, Directrice juridique de l'Agence des Systèmes d'Information Partagés de santé (ASIP santé)

– SEPTEMBRE 2018 –

Master 2 Droit de la Santé

Parcours « Droit et éthique des professions et des institutions de santé »

Continuité entre protection juridique de la personne et protection juridique des données de santé

Par Sophie LAMOUR

Sous la direction de Madame Florence EON

Directrice juridique de l'Agence des Systèmes d'Information Partagés de santé

Membres du jury :

- Monsieur Benoît APPOLIS, Maître de conférences en droit public à la Faculté de droit de l'Université de Rennes 1
- Madame Florence EON, Directrice juridique de l'Agence des Systèmes d'Information Partagés de santé (ASIP santé)

– SEPTEMBRE 2018 –

Remerciements

Je tiens à exprimer ma reconnaissance à mon Directeur de mémoire, Madame EON, Directrice juridique de l'ASIP santé, pour son accompagnement et ses conseils.

Je remercie Madame le Professeur MOQUET-ANGER ainsi que tous les professeurs de ce Master « Droit de la santé » pour leurs enseignements délivrés au cours de cette année.

Mes remerciements s'adressent également à Madame MAILLOUX, Responsable qualité au Centre Hospitalier de Dinan, et Madame PARTHENAY, Directrice adjointe au Centre Hospitalier de Montfort-sur-Meu et Saint-Méen-Le-Grand, et leur équipes respectives qui m'ont accueilli chaleureusement en stage et pris le temps de répondre à mes questions diverses.

Enfin, je remercie également mes proches, pour leur patience et leur aide dans l'élaboration de ce mémoire mais également tout au long de mon parcours universitaire.

À ma mère,

Sommaire

INTRODUCTION.....1

PARTIE I – Une législation sur la protection des données de santé influencée par celle des droits de la personne.....7

CHAPITRE I – Les droits fondamentaux de la personne.....8

SECTION I – La volonté de la personne.....9

SECTION II – La vie privée de la personne.....16

CHAPITRE II – Une protection renforcée, des garanties similaires.....23

SECTION I – Des principes déterminants autour de la prise en charge et du traitement.....24

SECTION II – Encadrement par des autorités spécialisées.....30

PARTIE II – Des différences croissantes remettant en cause la continuité ?.....36

CHAPITRE I – Des particularités propres aux données.....37

SECTION I – La question de la propriété des données.....38

SECTION II – La dématérialisation des données.....45

CHAPITRE II – Quelle protection des données pour l'avenir ?.....52

SECTION I – La pertinence d'un renforcement de la protection des données de santé semblable à la protection de la personne ?.....53

SECTION II – Vers une rupture de continuité ?.....59

CONCLUSION.....66

Liste des abréviations

AAI	Autorité administrative indépendante
ACS	Aide complémentaire santé
ALD	Affection de longue durée
ANAES	Agence nationale d'accréditation et d'évaluation en santé
ANSSI	Agence nationale de la sécurité des système d'information
API	Autorité publique indépendante
CASS	Cour de Cassation
CCNE	Comité Consultatif National d'Éthique
CE	Conseil d'État
CEDH	Cour Européenne des droits de l'Homme
CIL	Correspondant Informatique et libertés
CJA	Code de justice administrative
CMUC	Couverture maladie universelle complémentaire
CNEDIMTS	Commission nationale d'évaluation des dispositifs médicaux et technologies de santé
CNIL	Commission nationale de l'informatique et des libertés
CNOM	Conseil national de l'Ordre des médecins
CNS	Conférence nationale de santé
COFRAC	Comité français d'accréditation
CSP	Code de la Santé Publique
DM	Dispositif médical
DMP	Dossier médical partagé
DPO	Data protection officer (Délégué à la protection des données)
GEE	Groupe européen d'éthique
HAS	Haute autorité de santé
IA	Intelligence artificielle
INDS	Institut National des Données de Santé
IQSS	Indicateurs de qualité et de sécurité des soins
JO	Journal Officiel
NTIC	Nouvelles technologies de l'information et de la communication
OMS	Organisation mondiale de la santé
ONU	Organisation des Nations unies

PMSI	Programme de médicalisation des systèmes d’information
REP	Recours pour excès de pouvoir
RGPD	Règlement général sur la protection des données
RPB	Recommandations de bonnes pratiques
SADM	Système d’aide à la décision
SNDS	Système national des données de santé
SNIIRAM	Système national d'information inter-régimes de l'Assurance maladie
VIH	Virus de l'immunodéficience humaine

INTRODUCTION

« Une technologie sans éthique et sans connaissance équivaut à un corps sans âme et sans esprit" »[1] Monsieur J. BERANGER illustre ici les liens étroits entre la technologie et la personne.

Selon le dictionnaire de l'Académie Française, la protection vient du latin « *protectio* », dérivé de « *protectum* » signifiant « *toit, toiture* ». C'est l'« *action de protéger, de défendre quelqu'un contre les menaces, les dangers, de veiller sur lui.* ». C'est également, selon le dictionnaire Larousse, « *réclamer la protection des lois* ». La protection juridique se réfère alors aux moyens légaux permettant la mise en œuvre la dite protection.

La protection juridique de la personne peut porter tant sur la protection de son corps et de ses droits patrimoniaux que sur la protection de droits propres tel que les droits de la personnalité.

La protection du corps a pour but d'éviter les atteintes physiques au corps de la personne humaine. Les sources sont diverses. En effet, le Code pénal incrimine notamment les mutilations, blessures volontaires ou involontaires. Le Code de la Santé Publique (CSP) et les codes de déontologies des professions de santé assurent que l'acte médical ne porte pas une atteinte illégitime au corps.

La protection des droit patrimoniaux a pour but de protéger les biens matériels ou immatériels de la personne. A travers une réglementation que l'on retrouve principalement dans le Code Civil, la personne est in fine le sujet de la protection. Par exemple, des mesures intimement liées à l'individu peuvent être mis en place comme des mesures de tutelles. En fonction de l'intensité des délégations, les droits patrimoniaux seront alors sous la protection d'un tiers, dans le but de protéger l'individu concerné.

1 "La valeur éthique de la donnée de santé à caractère personnel : vers un nouveau paradigme de l'écosystème medical dématérialisé" de Jérome BERANGER, Chercheur en éthique du numérique

Enfin, les droits de la personnalité sont des droits intimement liés à la condition humaine, des droits considérés comme « naturels » aux hommes. Ce sont des droits plus abstraits. Il comprend le droit à la vie privée, le droit à l'image, le droit à l'honneur, le droit de s'opposer au traitement de données nominatives, les secrets de l'instruction et professionnels etc..

En somme, la protection juridique de la personne est une expression large. De nombreuses acceptions peuvent découler de cette notion.

Qu'est-ce qu'une *donnée* ? Selon le Dictionnaire de l'Académie française, une donnée est « la représentation d'une information sous une forme conventionnelle adaptée à son exploitation ». Elle devient une information si un processus de décodage se met en place. Pour autant, la donnée est en tant que telle brute, est une description élémentaire. Selon l'article 4 du Règlement Général sur la Protection des Données (RGPD), une donnée peut être à caractère personnel lorsque elle permet à une personne physique d'être identifiée ou identifiable. Une liste non exhaustive d'éléments permettant l'identification directe ou indirecte suit cet article. On y retrouve par exemple un nom, un numéro d'identification, identifié génétique etc.

La donnée sensible est quant à elle l'« *Information concernant l'origine raciale ou ethnique, les opinions politiques, philosophiques ou religieuses, l'appartenance syndicale, la santé ou la vie sexuelle. En principe, les données sensibles ne peuvent être recueillies et exploitées qu'avec le consentement explicite des personnes*. »[2]

La définition des *données de santé* a évolué. En 1997 la Commission Nationale de l'informatique et des libertés définissait les données de santé comme « des données individualisées recueillies auprès des professionnels de santé et relatives à leurs prescriptions et à leur pratique médicale »[3]. Le Conseil de l'Europe, à la même époque, avait quant à lui utilisé le terme de « données médicales ». Ce sont « toutes les données à caractère personnel relatives à la santé d'une personne, aux données ayant un lien

2 https://www.cnil.fr/fr/definition/donnee-sensible

3 CNIL 4 févr. 1997, portant adoption d'une recommandation sur le traitement des données de santé à caractère personnel: délibération n° 97-008

manifeste et étroit avec la santé ainsi qu'aux données génétiques »[4].

En 2010, une définition plus large est apportée par la Conférence nationale de santé. Celle-ci considère que les données de santé sont « des informations sur l'état de santé et les maladies d'un individu ou d'une population donnée mais aussi sur des éléments qui peuvent déterminer l'état de santé et les maladies (facteurs de risques médicaux, biologiques ou génétiques; comportements de santé; consommation des soins; positions sociales; conditions de travail; conditions de vie; environnement physique de l'habitat...) ».[5]

En 2018, le règlement européen sur la protection des données énonce dans son article 4 que « les données concernant la santé » sont les « 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 révèlent des informations sur l'état de santé de cette personne »[6]. C'est la première définition officielle que l'on retrouve dans un texte.

La *protection juridique des données de santé* est le droit des données de santé. Il existe deux corps de règles différents mais complémentaires. D'abord, le droit général des données personnelles se dédouble avec d'une part le RGPD et d'autre part avec la Loi Informatique et Liberté. Ensuite, il y a le droit spécial des données de santé qui lui aussi va se dédoubler. D'une part, avec les dispositions du CSP en particulier issues de la loi 2016 et d'autre part, avec la loi informatique et liberté.

En somme, la protection juridique des données de santé est encore émergente et fait l'objet de nombreuses évolutions récentes.

La continuité provient étymologiquement du latin « *continuus »,* « continu », de « *continere »,* « tenir ensemble » qui est le fait d'être continu ou continuel, de ne pas s'interrompre ou de ne s'interrompre que momentanément[7]. En l'espèce, la continuité va se traduire ici comme le lien entre d'une part le régime de protection de la personne et le

4 Comité des ministres, annexe à la Recommandation n° R(97) 5 du 13 février 1997 relative à la protection des données médicales

5 CNS, avis, 19 octobbre 2010 sur les données de santé informatisées

6 Art. 4 du RGPD

7 Selon le Dictionnaire de l'Académie Française

régime de protection des données. Dans ce contexte, elle sera *ou elle es*t l'esprit des lois correspondantes.

Les premières réglementations des données de santé sont apparues en 1978 en France. Les propos suivants s'appuient donc sur les législations et les pratiques de cette date à aujourd'hui.

Dans ce dossier, il faut entendre sous la notion de protection de la personne les définitions précitées à l'exception des mécanismes de protection du droit patrimonial, cette conception n'étant pas l'objet de mon propos.

La protection de la personne doit être interprétée majoritairement dans le contexte médical.

Enfin, il convient d'utiliser la dernière définition des données de santé instauré par le RGPD. Ainsi, une vision large des données doit irriguer cette analyse.

L'intérêt de la réflexion porte sur l'analyse des points communs et des différences entre les principes juridiques fondamentaux des deux régimes de protection. Le droit des données est encore en conception et a été influencé par les principes majeurs de la protection des personnes.

Dans cette matière, il y aura toujours l'enjeu de la conciliation entre les libertés et droits fondamentaux et l'intérêt général. Il conviendra d'analyser où se place le curseur entre les deux au fil des évolutions législatives.

Avec les dernières évolutions du régime de protection juridique des données de santé, existe-t-il encore une continuité dans la philosophie de la loi avec le régime de protection juridique des personnes ?

La France était un des pays précurseur dans la régulation juridique des données. Dès 1978, la première loi qui consacre la protection juridique des données a vu le jour, la loi n°

78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. Cette loi est née d'un projet du gouvernement de l'époque d'instituer une large base de donnée nationale dite « *SAFARI* », acronyme de « *Système Automatisé pour les Fichiers Administratifs et le Répertoire des Individus* ». Suite à la révélation du projet par Monsieur Philippe BOUCHER en 1974 dans le journal « *Le Monde* », ce projet a été fortement critiqué[89]

La loi introduit la notion de données à caractère personnel. Elle a institué des principes fondamentaux pour leur protection. Cette loi est de portée générale, elle ne concerne pas seulement les données de santé. Par ailleurs, c'est avec cette loi que la CNIL est crée comme autorité de contrôle. En 2004, la législation a été modifiée par la loi relative à la protection des personnes physiques à l'égard des traitements de données à caractère[10]. Cette loi est la transposition de la directive européenne 95/46/CE relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données. Elle modifie ainsi le cadre juridique initial. En somme, les données personnelles ne doivent pas être soumises à un traitement automatisé, sauf si celui-ci remplit les exigences posées par trois principes: proportionnalité, transparence, et finalité légitime. Des droits sont rapidement posés tels que le droit d'accès et de rectification aux données, le principe du consentement, le droit d'information etc. Une déclaration à la CNIL doit être effectué en cas de traitement ou stockage de données.

Il faut attendre 2016 pour que des changements importants surviennent dans le régime de protection des données de santé via deux lois.

D'une part, la loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé, dite loi Touraine, développe l'accès aux données de santé à des fins conditionnées (de santé publique, de recherche et d'innovation). Elle est à l'origine de l'Institut national des données de santé (INDS). Elle développe également la notion de « secret médical partagé » au sein de l'équipe de soins ou encore le droit à l'oubli pour les anciens malades

8 http://www.senat.fr/evenement/archives/D45/context.html

9 Voir Annexe n°1

10 Loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés

du cancer.

D’autre part, il y a la loi n° 2016-1321 du 7 octobre 2016 pour une République numérique dite la loi Le Maire. Cette loi étend l’obligation d’information à la personne. Depuis cette loi, la CNIL a prononcé des amendes à hauteur de 3 millions d’euros. Elle crée un droit à l’oubli et le droit à l’autodétermination informationnelle. Elle est également dans une politique d’ouverture des données publiques.

La dernière évolution est le règlement 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 connu comme le Règlement Général sur la Protection des Données. C’est l’aboutissement d’un travail d’une durée de 6 ans. La loi de 2004 anticipe d’ailleurs sa mise en application. Ce règlement est entré en vigueur le 25 mai 2018. Il renforce la protection des citoyens et de leurs données notamment par l’apparition de nouveaux droits tels que la portabilité des données. De plus, il accroît les responsabilités pour les acteurs des traitements de données, il défini les conditions pour le transfert de données personnelles hors de l’Union Européenne.

Enfin, un code des données personnelles 2018-2019 est prévu pour septembre 2018. Ce code sera l’agrégat de différents textes majeurs précités mais aussi, des textes plus spécifiques propres à certains domaines tel que les assurances, le travail ou encore la santé.

La première partie de cette étude portera sur l’influence des droits de la personne sur la protection des données de santé (PARTIE I). Par la suite, la constatation de différences croissantes questionne la réelle continuité entre les deux régimes de protection (PARTIE II).

PARTIE I – Une législation sur la protection des données de santé influencée par celle des droits de la personne

« *L'informatique doit être au service de chaque citoyen. […] Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques. [...]* »[11].

Le scandale du projet SAFARI a été l'un des premiers débat national autour des droits de l'homme et des nouvelles technologies. Le projet ayant été jugé trop attentatoire aux droits et libertés fondamentaux, celui-ci a été abandonné.

Soucieux des risques que peuvent entraîner le recueil et le traitement de données personnelles, les français ont par conséquent opté pour un modèle de protection des données influencé par les droits de la personne. C'est pourquoi l'article 1 susvisé de la loi « Informatique et Libertés » rappelle symboliquement l'importance d'une conciliation entre les droits de la personne et l'essor des nouvelles technologies.

Afin de protéger au mieux les données de santé, les mécanismes juridiques traditionnels que l'on retrouve parmi les droits fondamentaux de la personne (CHAPITRE I) ont été adaptés. Un écho se retrouve également dans des dispositifs de protection particuliers que l'on peut retrouver dans le droit de la santé (CHAPITRE II).

11 Art. 1er de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

CHAPITRE I – Les droits fondamentaux de la personne

Selon la formule du Conseil D'État, « *L'essor du numérique a suscité la reconnaissance de nouveaux droits fondamentaux et modifié leurs conditions d'exercice* »[12].

L'expression « *droits fondamentaux* » est dérivée du droit allemand. Son contenu est encore souvent débattu par les juristes. Cependant, la doctrine s'accorde pour considérer que les droits fondamentaux sont inhérents à la notion même d'homme et que l'État est l'organisme garant de l'effectivité de ces droits[13]. Ils sont d'une normativité plus importante que d'autres droits puisqu'ils sont généralement de valeur constitutionnelle. Pour autant, il n'existe toujours pas de catalogue des droits fondamentaux malgré des demandes dans ce sens[14]. Il est communément admis que cette notion englobe les droits de l'Homme, les libertés publiques ainsi que des droits particuliers tels que des droits procéduraux.

Dans l'intérêt du propos, nous allons principalement faire la focale sur l'autonomie de la volonté de la personne (SECTION I) ainsi que son droit au respect de la vie privée (SECTION II).

12 Rapport du Conseil d'Etat "Le numérique et les droits fondamentaux"

13 "La terminologie des "droits fondamentaux" dans la jurisprudence du Conseil Constitutionnel" du Pr. Samuel ETOA

14 Voir sur ce point JO Sénat du 21/10/1999 - page 3494

SECTION I – La volonté de la personne

Le respect de la volonté de la personne découle du respect de la dignité de la personne, principe fondamental dans notre état démocratique. Ce respect se manifeste par le recueil du consentement de la personne concernée par l'acte médical ou le traitement des données de santé (§1). Ce consentement ne peut intervenir valablement qu'une fois que l'information a été correctement délivrée (§2).

§1 – Le consentement

Au delà même de la recherche du consentement pour toute action (A), les deux régimes législatifs s'enquirent également à ce que l'individu soit partie intégrante dans sa prise en charge (B).

A – La recherche du consentement pour toute action

Selon le Lexique des termes juridiques 2017-2018, le consentement est « *dans la création d'un acte juridique, l'acceptation par une partie de la proposition faite par l'autre. L'échange des consentements entraîne l'accord de volonté qui lie les parties* ». Le consentement, pour être valide, doit être libre et éclairé. Ainsi, le consentement ne doit pas avoir été donné sous contrainte ou sous l'effet d'une altération mentale et l'individu doit avoir eu une information spécifique. De plus, le contrat ne doit pas être contraire à des dispositions d'ordre public. C'est une liberté fondamentale[15] qui découle du respect de la dignité humaine. Par ailleurs, selon la Cour Européenne des Droits de l'Homme, le consentement entre dans le champ de l'article 8 de la Convention Européenne des Droits de l'Homme[16].

En droit de la santé, un des principes majeurs est le principe du consentement avant tout acte médical. Il existait déjà avant la loi du 4 mars 2002 relative aux droits des malades et à la qualité du système de santé. En effet, c'était déjà un principe jurisprudentiel[17].On le

15 Selon le CJA, art. 512-2
16 CEDH, Codarcea c/ Roumanie du 2 juin 2009 31675/04
17 Cass., 28 janvier 1942, Parcelier c/ Teyssier

retrouve actuellement à l'article L.1111-4 du CSP. « *Aucun acte médical ni aucun traitement ne peut être pratiqué sans le consentement libre et éclairé de la personne et ce consentement peut être retiré à tout moment*". Le consentement avant tout acte médical suit également les caractéristiques classiques : il doit être libre et éclairé. Enfin, l'article précité précise bien que le consentement peut être retiré à tout moment, sans avoir besoin d'apporter une preuve quelconque.

C'est dans cette même vision que les données de santé, étant considérées comme des données sensibles, nécessitent en principe le consentement pour son recueil et son traitement. Le consentement est défini par l'article 2 de la Directive européenne sur la protection des données personnelles[18] comme «*la manifestation de volonté, libre, spécifique et informée par laquelle la personne concernée accepte que les données à caractère personnel la concernant fassent l'objet d'un traitement*». Cela traduit en pratique un acte positif, le consentement est dit exprès. La loi du 6 août 2004 a transposé indirectement cette définition. Or, la loi du 26 janvier 2016 de modernisation de notre système de santé apporte une nouvelle rédaction qui in fine modifie les modalités du consentement : « *Cet hébergement, quel qu'en soit le support, papier ou électronique, est réalisé après que la personne prise en charge en a été dûment informée et sauf opposition pour un motif légitime* »[19]. Il suppose désormais que la personne responsable du traitement délivre une information et que le patient n'oppose pas de motif légitime. Enfin, le consentement exprès a été gardé pour la création des dossiers médicaux. Ainsi, « *le dossier médical partagé est créé sous réserve du consentement exprès de la personne ou de son représentant légal »*[20]. La nécessité de ce consentement initial a d'ailleurs été remis en cause, notamment par la Cour des Comptes[21].

On remarque un certain parallélisme entre les deux régimes de protection, mais la portée du consentement reste plus faible au niveau des données, elle s'est étiolée au fil des années. Pour l'acte médical, le consentement ne le lie pas ad vitam aeternam. Pour les données, le consentement est majoritairement présumé et donc ne suppose donc pas

18 Directive européenne n°95/46/CE du 24 octobre 1995 sur la protection des données personnelles
19 Art. L1111-8 du CSP
20 Art. L. 1111-14 du CSP
21 Rapport public annuel 2018 de la Cour des Comptes : "les services publics numériques en santé"

d’acte positif de la personne. De plus, il est pertinent de s’interroger sur la notion de « motif légitime ». Puisque la loi n'apporte pas de définition, on se retrouve face à une problématique juridique. Elle sera alors définie au cas par cas. En tout état de cause, en l’absence de lisibilité, cette démonstration va être difficile pour les patients.

B – Le patient réel acteur de sa prise en charge

L’évolution des législations favorise la prise de décisions de l’individu concernant tant sa santé que ses données. Il y a eu une réelle rupture avec le paternalisme médical et une volonté d’éducation des citoyens pour les données. On est dans l’ère de l’ « empowerment » du patient.

Cette tendance est prégnante depuis la loi du 4 mars 2002. « T*oute personne prend, avec le professionnel de santé et compte tenu des informations et des préconisations qu'il lui fournit, les décisions concernant sa santé »*[22]*.* Le médecin est tenu de respecter le choix de la personne tant que les informations ont été correctement délivrées. Cette loi a eu la volonté de remettre le patient en tant qu’acteur principal de sa prise en charge. Cela est passé par le renforcement des droits du patient dont l’obligation de la délivrance d’une information spécifique. Ainsi, on passe d’un paternalisme médical à des solutions individuelles discutées avec le patient en vue d' un réel partenariat.

En parallèle, on retrouve ce mouvement concernant les données de santé notamment au travers du dossier médical partagé (DMP). C’est le patient lui même qui peut transmettre et afficher ce qu’il souhaite. Certaines informations peuvent être rendues inaccessibles par le titulaire du dossier médical partagé[23] et il peut également modifier la liste des professionnels ayant accès à son dossier[24]. Cependant, il ne peut altérer le contenu même de ce dossier[25]. Depuis 2002, le patient peut accéder directement à son dossier médical. sans avoir besoin d'un médecin pour faire le lien.

22 Art. L. 1111-4 du CSP
23 Art. L. 1111-15 du CSP
24 Art. L. 1111-19 du CSP
25 D. n° 2016-914 du 4 juillet 2016 relatif au dossier médical partagé, Article. R. 1111-36 CSP

On trouve également une réelle similitude sur les procédures d'anticipation du décès. D'une part, il y a l'existence des directives anticipées. Toute personne majeure peut rédiger des directives anticipées pour le cas où elle serait un jour hors d'état d'exprimer sa volonté[26]. Ces directives anticipées expriment la volonté de la personne relative à sa fin de vie en ce qui concerne les conditions de la poursuite, de la limitation, de l'arrêt ou du refus de traitement ou d'acte médicaux. Elle ont été renforcé en 2016 puisqu'elles sont désormais opposables. D'autre part, il y a la possibilité de prévoir sa « *mort numérique* »[27] depuis la loi « Pour une République numérique » du 7 octobre 2016. Cette loi permet à chacun de définir des directives relatives à la conservation, à l'effacement et à la communication de ses données à caractère personnel après son décès. Ces directives sont générales ou particulières.

Le processus « empowerment » est encore nouveau pour les données de santé. Le patient n'a pas, en droit et en fait, la pleine maîtrise de ses données de santé. Pour autant, les législations récentes vont dans le sens d'une plus grande responsabilisation.

§2 – Information et opposition

Dans les régimes juridiques de protection des données personnelles, il existe quatre principes cardinaux qui sont le droit d'information, le droit d'opposition, le droit d'accès et le droit de rectification. La comparaison avec les principes fondamentaux n'est pertinente que sous l'angle du droit d'information (A) et du droit d'opposition (B).

A – Le droit d'information

Le droit d'information n'a cessé de se développer dans tous les domaines du droit. On le retrouve en droit médical à l'article L1111-2 du CSP. « *Toute personne a le droit d'être informée sur son état de santé* ». C'est la condition *sine qua non* afin que l'individu donne un consentement effectivement éclairé. La Cour de cassation rappelle que ce principe découle lui aussi du respect de la dignité de la personne humaine[28]. Les ordres

26 Art. L. 1111-11 du CSP
27 Art. 40-1 de la loi "informatique et libertés"
28 Cass., Civ 1re, 9 oct. 2001, 00-14.564

professionnels de santé l'avaient déjà intégré dans leurs codes de déontologies respectifs. Par la suite, il a été consacré dans le CSP avec la loi du 4 mars 2002.

On retrouve également l'obligation d'information préalable au traitement des données à l'article 13 du règlement européen de protection des données. C'était déjà le cas avec l'article 32 de la Loi Informatique et Libertés. Plusieurs items doivent être communiqués à l'individu concerné dont notamment l'identité du responsable du traitement, la finalité poursuivie, les droits qu'elle tient, de la durée de conservation etc..

La délivrance de l'information doit répondre à des caractéristiques. Dans le droit médical, selon la jurisprudence, l'information doit être «loyale, claire et appropriée»[29]. Le patient doit être informé des risques dans des conditions qui permettent de recueillir son consentement éclairé[30]. Pour les données, l'Information doit être fournie « d'une façon concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples » selon l'article 12 du Règlement européen sur la protection des données. De même, l'obligation doit être faite à chaque nouvel acte[31] ou traitement. La délivrance de l'information médicale suppose un rendez-vous individuel. A contrario aucun texte n impose un tel rendez-vous pour le traitement des données,

La charge de la preuve appartient, dans les deux régimes de protection, au professionnel qui a le devoir d'information[32]. Les préjudices réparables liés au défaut d'information sont à ce jour plus développés concernant la responsabilité médicale[33].

B – Le droit d'opposition

Le droit d'opposition s'exprime en droit médical par le droit au refus de soins, au refus de traitement. Le médecin ne peut pas contourner ce choix selon l'Article. L. 1111-4 «Le médecin a l'obligation de respecter la volonté de la personne après l'avoir informée des conséquences de ses choix et de leur gravité.[...]». Cependant, il y a toujours l'obligation

29 Cass., Civ. 1re, 14 octobre 1997, n° 9519609
30 CE, sect., 5 janvier 2000, Cts Telle et AP-HP, n° 181899
31 CAA, Douai, 30 juin 2010 n° 09DA00054
32 Cass., Civ. 1re, 25 février 1997, Hedreul c/ Cousin sur l'abandon de la "preuve diabolique"
33 Sur ce point, voir le manuel "Droit hospitalier" du Pr. MOQUET ANGER, 5ème édition, LGDJ

déontologique de porter assistance à personne en péril à l'article R. 4127-9 du CSP. S'il ne porte pas assistance dans une telle situation, il peut engager sa responsabilité pénale selon l'article 223-6 du Code pénal pour l'infraction de non-assistance à personne en péril.

Avant la loi de 2002, le Conseil d'État avait admis la possibilité de contourner le refus d'un patient en validant le fait que l'équipe médicale procède à une transfusion sanguine sans le consentement de l'intéressé afin de lui sauver la vie[34]. Avec les avancées législatives, cette jurisprudence semble obsolète. A terme, le médecin doit s'incliner à la décision de refus s'il celle-ci est réitérée dans un « délai raisonnable »[35].

Pour les données personnelles, le droit d'opposition est apparu avec la Loi Informatique et Libertés. Article 38 « Toute personne physique a le droit de s'opposer, pour des motifs légitimes, à ce que des données à caractère personnel la concernant fassent l'objet d'un traitement. » Le droit d'opposition est conditionné (sauf en cas de prospection commerciale), il n'est pas absolu comme le droit de refus de soins. Ceci est d'autant plus recevable lorsqu'il s'agit d'une obligation légale de traitement. Une nouvelle fois, le législateur ne précise pas ce qu'il faut entendre par « motifs légitimes ». Le RGPD a substitué cette formule par « des raisons tenant à une situation particulière » sans y apporter plus de précisions[36]. Ce sera à la jurisprudence de définir les critères d'un refus légitime.

Si on pousse la logique plus loin, le droit d'opposition peut aussi s'exprimer au travers du droit de ne pas tout dire à son médecin. Ce choix est possible au nom du respect de l'intimité du patient. Cette possibilité se retrouve dans le droit spécial des données de santé avec le « droit au masquage ». On retrouve ce droit à l'article 38 de la la loi Informatique et Libertés Dans les deux cas, le patient doit être informé des conséquences possibles de son manque de transparence.

La loi du 26 janvier 2016 précise les règles de responsabilité en cas de préjudice lié au

34 Voir CE, Ass., 26 oct. 2001 Madame Senanayake

35 Sur le délai raisonnable, voir le manuel "Droit hospitalier" du Pr. MOQUET ANGER, 5ème édition, LGDJ, p358-362

36 Art. 21 du RGPD

masquage. Selon l’article L. 1111-15 « La responsabilité du professionnel de santé ne peut être engagée en cas de litige portant sur l'ignorance d'une information qui lui était masquée dans le dossier médical partagé et dont il ne pouvait légitimement avoir connaissance par ailleurs ».

SECTION II – La vie privée de la personne

Selon l'article 9 du Code civil, « *chacun a droit au respect de sa vie privée* ». Ce principe a en France une valeur constitutionnelle[37]. Elle découle du respect de la dignité et de l'intimité des personnes. En l'espèce, le respect de la vie privée va se décliner sous l'angle de la confidentialité des informations (§1) et de la non discrimination (§2).

§1 – La confidentialité

La confidentialité est l'un des points les plus sensibles dans les deux régimes. Elle recouvre le secret des informations (A). Pour autant, le secret médical s'avère être l'objet de plus en plus d'exceptions (B).

A – Le secret des informations

Le secret des informations est l'une des pierres angulaires du droit médical. Comme le Professeur PORTES le soulignait « *il n'y a pas de médecine sans confiance, de confiance sans confidence et de confidence sans secret* ». Le secret a été institué en premier lieu dans l'intérêt du malade. Avant la loi de 2002, les médecins utilisaient la notion de secret médical à l'encontre du patient[38]. Aujourd'hui, on le retrouve à l'article L.1110-4 du CSP l'affirmation du « *droit au respect de sa vie privée et des informations la concernant* ». L'obligation de confidentialité, du secret des informations est plus large que le secret médical. Il couvre des informations non médicales et ne s'impose pas qu'aux médecins mais aussi aux professions de santé.

La protection des données rentre dans le champ de l'article 8 de la CEDH, (respect de la vie privée). Dans la loi Informatique et Libertés, on ne retrouve pas le terme de droit au respect de la vie privée mais il est entendu dans l'article 7 : un traitement ne doit pas méconnaître les droits fondamentaux. Pour autant, un traitement automatisé n'implique pas automatiquement une violation de la vie privée. De plus, il y a une obligation de

37 Cons. Const., décision n° 76-75 DC, 12 janvier 1977

38 Voir "Secret médical et loi du 4 mars 2002 : quels changements?" par Dominique THOUVENNIN, Laennec, 2007/1 pages 23-37

sécurité des informations détenues[39]. Cette question est d'autant plus cruciale que les systèmes d'information partagés en santé sont en essor. Cela nécessite une sécurité adaptée de manière à assurer la confidentialité des données de santé. Afin d'éviter l'accès de ces informations à des tiers, il existe une politique générale de sécurité des systèmes d'information de santé (PGSSI-S) qui développe notamment un référentiel d'authentification des acteurs. C'est dans cet optique que le programme « Hôpital Numérique » s'inscrit. Les résultats restent mitigés malgré les efforts, ce qui pose la question de la réelle confidentialité des informations. [40]

Le secret médical s'impose à tous les médecins. Le secret des informations des données s'impose quant à lui au responsable du traitement. Dans les établissements de santé, le responsable est le directeur d'établissement. Il doit ainsi prendre les mesures nécessaires pour garantir cette confidentialité. Cela peut s'effectuer par la mise en place d'habilitation ou de modifications des mots de passes régulièrement.

Le secret médical est absolu notamment à l'égard de personnes privées sensibles telles que l'employeur ou l'assureur. Il « *couvre tout ce qui est venu à la connaissance du médecin dans l'exercice de sa profession, c'est-à-dire non seulement ce que lui a confié son patient, mais aussi ce qu'il a vu, entendu ou compris* » selon l'article 4 du code de déontologie médicale (article R.4127-4 du CSP)[41]. Le secret des données de santé ne concerne que ce qui a été effectivement transmis.

Dans les deux cas, le secret est renforcé pour le mineur. D'un coté, le mineur a un réel droit au secret médical notamment à l'égard de ses parents ; de l'autre, une politique du droit à l'oubli plus favorable[42].

B – Vers affaiblissement du secret médical ?

Au fil des révisions, les exceptions au secret médical se sont développées. Dès 1994, le

39 Art. 34 de la loi "informatique et libertés"
40 Voir "Bilan du programme Hopital Numérique 2012/2017" sur http://solidarites-sante.gouv.fr/
41 CE, 15 décembre 2010, n°330314
42 Art. 40 de la loi "informatique et libertés"

Code pénal[43] en développe deux :

- L'information de sévices ou de privations infligés à un mineur de moins de quinze ans ou à une personne qui n'est pas en mesure de se protéger ;
- L'information, avec l'accord de la victime, au Procureur de la République des sévices qu'il a constaté et qui lui permettent de présumer que des violences sexuelles ont été commises.

Dans de nombreuses circonstances, le législateur a prévu la divulgation de certaines informations relatives à l'état de santé des personnes, afin de permettre l'application d'une loi. On y retrouve notamment la déclaration des maladies professionnelles et des accidents du travail ou encore la déclaration des maladies contagieuses.

Plus récemment, le développement des systèmes d'information partagés vient également porter un coup au devoir de confidentialité. La notion de secret partagé a été consacré avec la loi 2016. Il permet d'échanger des informations personnelles sur le patient entre toute l'équipe médicale tant que le patient n'exprime pas son opposition. Les informations délivrées par le patient sont considérées comme confiées à l'ensemble de l'équipe de soin. Un seuil est prévu pour éviter toute divulgation disproportionnée : la communication doit être limitée aux seules informations nécessaires à sa prise en charge[44]. Ces nouveautés ont posé question de la définition de l'équipe de soin. Celle-ci ne se limite plus aux équipes de l'hôpital. Des acteurs extérieurs sont compris tel que du personnel du secteur social et médico-social. Le secret médical traditionnel, c'est-à-dire inhérent au « *colloque singulier* », s'est transformé en un secret partagé, plus proche de la réalité du terrain des équipes.

De même, la loi du 26 janvier 2016 a étendu les possibilités de communication aux hypothèses de diagnostic d'une maladie infectieuse transmissible ou à la nécessité de se défendre en justice.

Est-il nécessaire d'affaiblir la portée du secret médical afin d'améliorer les prises en charge et les parcours de soins ? Cette question est un enjeu de continuité des soins.

43 Art. 226-14 du Code pénal
44 Art. L. 1110-4 du CSP

C'est en tout cas la raison pour laquelle le « *secret médical partagé* » a été développé. La nécessité de s'adapter au nouvelles formes d'exercice passe parallèlement par l'adaptation de certains principes. De même, afin de compenser à ces nécessités, il faut encadrer la qualité et la sécurité des pratiques professionnelles. Ex : Fermeture des sessions, ne pas laisser des dossiers ouverts sans surveillance...

S'il y a divulgation du secret médical, la responsabilité civile et pénale du professionnel pourra être engagée. Est-ce que la politique jurisprudentielle va devenir plus favorable aux professionnels en cas de litige autour de la confidentialité des informations ? Cela semble peu probable. Bien qu'il y ait une tendance à l'accroissement des dérogations strictement encadrées, l'interdiction de divulgation des informations de santé reste un principe fondamental.

§2 – Le principe de non-discrimination

Le principe de non-discrimination s'applique tant dans l'action de donner des soins que dans le traitement des données de santé (A). De plus, découlant de ce principe, le droit à l'oubli prend de plus en plus d'ampleur (B).

A – Le principe

Selon l'article premier de la Déclaration Universelle des Droits de l'Homme (1948), « *Tous les êtres humains naissent libres et égaux en dignité et en droit [...]* ». C'est un principe à valeur constitutionnelle. Les discriminations interdites sont listées par les articles 225-1 et suivants (sexe, âge, religion, etc.)

Les professionnels de santé et les établissements ont une obligation d'égalité de traitement. Cela vient au soutien de l'égal accès aux soins. Comme le souligne Madame Le Professeur MOQUET-ANGER, « *si prise en charge du patient différencié en vertu de critères autres que médico-scientifiques, l'égalité disparaît* »[45]. Dans le prolongement, les professionnels de santé sont soumis au devoir d'impartialité et à l'obligation de neutralité.

45 Voir le manuel "Droit hospitalier" du Pr. MOQUET ANGER, 5ème édition, LGDJ, page 339, paragraphe 377.

Cette interdiction de discrimination se retrouve également dans les codes déontologiques des professionnels de santé[46]. En effet, à l'article R. 4127-7, il est précisé que le médecin doit avoir une prise en charge « *avec la même conscience toutes les personnes* [...] ». La pratique discriminatoire est donc également une faute disciplinaire.

L'ONU a relevé en 2017 que ce sont les « populations marginalisées et stigmatisées de la société » qui font l'objet des discriminations dans les établissements de santé[47]. Par cette expression, il faut entendre notamment les personnes atteintes du VIH, les populations autochtones ou encore les réfugiés. Ainsi, pour améliorer la prise en charge de ces patients, l'ONU préconise en autre une sensibilisation appuyée complétée par une formation des agents sur cette problématique.

Concernant le traitement de données, celui-ci ne doit pas entraîner de discriminations. La liste des données sensibles dont le traitement est en principe interdit, rejoint les notions évoquées à l'article 225-1 du Code pénal. De plus, l'article 25 de la loi Informatique et Libertés dispose que « les traitements automatisés susceptibles, du fait de leur nature, de leur portée ou de leurs finalités, d'exclure des personnes du bénéfice d'un droit, d'une prestation ou d'un contrat en l'absence de toute disposition législative ou réglementaire » sont soumis à autorisation préalable de la CNIL.

Ce risque de discrimination était l'un des plus décrié avec le projet SAFARI. Aujourd'hui il reste un enjeu fondamental pour les données sensibles, Cette préoccupation avait d'ailleurs été soulignée par le GEE dès 1999[48]. Il avait déjà informé du risque discriminatoire possible : « *L'informatisation des données a pour conséquence la mondialisation des standards et des procédures [...], standardisation qui n'est pas neutre car elle se traduit par des choix éthiques, sociaux, politiques et épistémologiques qui peuvent être source de discrimination* ».

46 "Les sources du droit médical" par Madame TINOT-THOMAS, Thèse de 2004

47 Conseil de Coordination du Programme de l'ONUSIDAUNAIDS/PCB (41)/17.27

48 Voir avis GEE n°13 "Aspects éthiques de l'informatisation des données de santé dans la société de l'information du 30 juillet 1999"

B – Droit à l'oubli

Du principe de non-discrimination découle le droit à l'oubli. Cette notion a fait l'objet de nombreuses interprétations. Pour certains c'est un droit à l'intimité, ou encore un droit qui se rapproche de l'autodétermination informationnelle. La conception restreinte peut se définir comme la suppression automatique de données après l'écoulement d'un délai fixé préalablement. Autrement dit, le droit à l'oubli numérique consiste seulement en la disparition d'informations. Le déréférencement fait partie des moyens d'actions pour mettre en œuvre le droit à l'oubli. Ce dernier permet de supprimer des résultats de recherche associés au nom et prénom mais le contenu original reste inchangé. Une procédure distincte sera nécessaire pour effacer les informations directement avec l'hébergeur.

Par ailleurs, la Cour de Justice de l'Union Européenne indique que le droit à l'oubli prévaut sur les intérêts des hébergeurs.[49] Pour autant, selon le bilan de Google, un peu moins de la moitié des demandes de droit à l'oubli aboutissent depuis 2014[50] . Cela pose la question de la réelle effectivité du droit à l'oubli.

La loi 2016 a consacré ce droit en matière médicale. Il vient encadrer l'accès au crédit des personnes avec un fort risque de santé : elle limite les majorations excessives et limite l'accès aux informations. Concrètement, les anciens malades du cancer n'auront plus à déclarer leur ancienne pathologie passé un délai qui est en principe de dix ans après la fin de leur traitement (et sans rechute). Ils peuvent donc à l'issu de ce délai souscrire à un contrat d'assurance sans surprime, ni exclusion de garantie. Autrement dit, ils auront les mêmes conditions que les personnes n'ayant pas été malade. Une convention dite AERAS a été signé en 2006 avec une entrée en vigueur en 2007. Les avenants ne cessent d'élargir le champ de couverture des risques aggravés de santé. Cette convention a d'ailleurs été révisée suite à l'introduction au droit à l'oubli. Une grille de référence a été élaborée afin de mettre en œuvre le droit à l'oubli. Celle-ci sera régulièrement révisée en fonction des avancées thérapeutiques.

49 CJUE, 13 mai 2014, C-131/12
50 http://transparencyreport.google.com/eu-privacy/overview

Pour le traitement des données de santé, il y a un principe de conservation limitée des données. Celles-ci ne peuvent être conservées dans les fichiers au-delà de la durée dite « *nécessaire à la réalisation de la finalité poursuivie* ». On retrouve cette norme à l'article 5 du Règlement général sur la protection des données. C'est au responsable du traitement de fixer une durée de conservation raisonnable . Le code pénal sanctionne la conservation des données pour une durée supérieure à celle qui a été déclarée de 5 ans d'emprisonnement et de 300 000 € d'amende.[51]

Par exemple, la limite de conservation d'un dossier médical dans un cabinet médical libéral est fixé à 10 ans[52], celle d'un dossier médical dans les établissements de santé est fixé 20 ans à partir du dernier passage dans l'établissement par le patient ou 10 ans à partir de la date du décès[53].

51 Art. 226-20 du Code Pénal
52 Art. L.1142-28 du CSP
53 Art. R. 1112-7 du CSP

CHAPITRE II – Une protection renforcée, des garanties similaires

La matière médicale n’est pas anodine, elle est l’une des plus régulée. En quelques années, le CSP a doublé voir triplé de volume. Bien que le droit des NTIC soit encore jeune, la volonté d’’une réglementation particulière se manifeste déjà.

Ainsi, au delà du respect de normes intemporelles et supra-législatives, de nombreux instruments de régulation traditionnels sont identiques. Les outils juridiques du droit médical pour assurer une garantie renforcée se retrouvent dans le droit des données.

Pour ce faire, se sont développés pour le droit des données des principes et des garanties similaires (SECTION I). De même les deux matières sont encadrées par des autorités spécialisées (SECTION II).

SECTION I – Des principes déterminants autour de la prise en charge et du traitement

Afin de pouvoir légitimer certains actes médicaux et traitements de données sensibles, des principes ont permis de les encadrer afin de pouvoir justifier de telles dérogation (§1). Pour autant, tout au long du processus, l'acte doit toujours répondre à des critères de finalité et de proportionnalité (§2).

§1 – Les principes autour de la justification de l'acte

Le principe est l'interdiction générale d'une part d'exercer une atteinte sur la personne et d'autre part de traiter des données dites sensibles (A). De plus, la notion de loyauté doit également être présente avant même l'acte médical et la collecte de données (B).

A – Le principe d'interdiction générale d'atteinte à la personne et de traitement données sensibles

Depuis 1994, l'article 16 du Code Civil dispose que « l*a loi assure la primauté de la personne, interdit toute atteinte à la dignité de celle-ci et garantit le respect de l'être humain dès le commencement de sa vie* ». C'est le principe de dignité qui permet d'interdire que l'être humain soit considéré comme sujet d'expérimentation. Le consentement de la personne ne change rien, cela relève d'une question d'ordre public.

Dans le droit médical, il y a le principe d'interdiction des atteintes à l'intégrité corporelle. Le corps est considéré comme inviolable. L'inviolabilité et l'intégrité corporelle sont deux notions intimement liées. Le principe d'intégrité est affirmé à l'article 16-3 du Code civil. Des exceptions sont prévues par ce même article : on peut porter atteinte au corps d'une personne s'il existe un intérêt médical direct pour la personne concernée ou dans l'intérêt thérapeutique d'autrui de manière exceptionnelle. Ces principes garantissent que l'individu ne peut pas consentir à des atteintes sur son corps. Le principe est tel que même la prothèse devient juridiquement une partie du corps[54].

54 "Droit de la personne – Leçon 6 : les droits relatifs au corps humain" du Pr. BINET, UNJF.

Pour les données, il y a l'interdiction de la collecte et du traitement des données dite sensibles. L'article 8 de la Loi Informatique et Libertés dispose que « *il est interdit de collecter ou de traiter des données à caractère personnel qui font apparaître, directement ou indirectement, les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou qui sont relatives à la santé ou à la vie sexuelle de celles-ci* ». C'est pourquoi, en principe, les données sensibles ne peuvent faire l'objet d'un traitement.

Liste d'exception prévu par la loi. Cette liste est limitative. On ne peut pas aller au-delà des cas prévus. On retrouve cette liste à l'article 8. Ne seront pas soumis à l'interdiction notamment :

- Les traitements consentis de manière exprès, sauf dans le cas où la loi prévoit que l'interdiction peut être levée par consentement ;
- Les traitements nécessaires à la sauvegarde de la vie humaine, mais auxquels la personne concernée ne peut donner son consentement par suite d'une incapacité juridique ou d'une impossibilité matérielle ;
- Les traitements portant sur des données à caractère personnel rendues publiques par la personne concernée ;
- Les traitements 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 prévue par l'article 226-13 du code pénal ;
- Les traitements statistiques réalisés par l'Institut national de la statistique et des études économiques ou l'un des services statistiques ministériels ;
- Les traitements nécessaires à la recherche dans le domaine de la santé ;
- L'intérêt public ;

L'anonymisation des données peut également, compte tenu de leur finalité, permettre que le traitement soit considéré comme licite.

B – Le principe de loyauté

La loyauté est le fait pour une personne de se conformer aux exigences de l'honneur et de la probité. Cela rejoint le concept de « *bonne foi* ». C'est une notion traditionnelle qui a une influence dans de nombreuses règles juridiques du droit français. Elle suppose l'absence d'abus ou d'intention de nuire. En somme, les deux régimes juridiques sont dans une politique de transparence.

Ce principe se retrouve tant dans la relation rapport médecin-patient, dans le colloque singulier, au travers de la confidentialité et la délivrance d'information. On retrouve cette norme notamment à l'article R.4127-35 du CSP : le médecin doit au patient une « *information loyale, claire et appropriée sur son état, les investigations et les soins* ». Sans l'accomplissement de cette exigence, le patient ne peut donner un consentement valable.

On retrouve le principe de loyauté dans le droit des données. Il rejoint le principe de licéité de la collecte. En effet, la loi impose un principe de loyauté dans l'utilisation des données. L'article 6 du RGPD dispose que « *les données [soient] collectées et traitées de manière loyale et licite* ». Cela implique l'information et consentement libre et éclairé sauf base légale alternative.

Dans le domaine non médical, un exemple de collecte déloyale a été jugé en 2006. Cela concernait un recueil d'adresses mails personnelles sur internet à l'insu des personnes concernées[55]. Dans le domaine médical, le principe de loyauté a inspiré la Haute Autorité de Santé pour un référentiel des bonnes pratiques dans le marché des applications mobiles e-santé. Afin que la collecte soit loyale, pour la Haute Autorité de Santé, de telles applications doivent donc être conçues afin que le consentement à l'accès et au partage de telles informations soit expresse [56].

55 Cass., com.,14 mars 2006, n°0583423

56 Référentiel de bonnes pratiques sur les applications et les objets connectés en santé (Mobile Health ou mHealth) de la Haute Autorité de Santé, Octobre 2016

§2 – Les principes autour des conditions de l'acte

Tant l'acte médical que le traitement des données doivent répondre à deux exigences. D'une part, il doit répondre à une finalité (A), d'autre part il doit être proportionnel à celui-ci (B).

A – Le principe de finalité

La finalité de l'acte de soin se traduit par le principe d'une nécessité médicale pour la personne ou à titre exceptionnel dans l'intérêt thérapeutique d'autrui. L'atteinte à l'intégrité du corps ne peut donc être pratiquée que selon ces deux finalités précises, c'est la condition de licéité. A l'origine, la finalité se définissait comme l'intérêt ou la nécessité thérapeutique[57]. La loi bioéthique de 1994 a repris le même terme. Ce n'est qu'en 1999 que l'expression « *nécessité thérapeutique* » a été modifié en « *nécessité médicale* ».

Par exemple, la Cour de cassation a déjà considéré que le principe de finalité n'était pas respecté pour une « *intervention chirurgicale mutilante, non justifiée et non adaptée* »[58]. Cependant, les décisions dans ce sens sont rares. Cette rareté peut être la traduction du fait que son contenu est trop large. Ainsi la protection par le principe de finalité perd de son intérêt.

Le principe de finalité s'applique également pour le traitement des données. En effet, il faut que la finalité soit déterminée et légitime. De plus, celle-ci doit être compréhensible pour les parties prenantes. La finalité représente l'intérêt légitime que le responsable du traitement doit poursuivre. Cela permet d'assurer que le but du traitement ne sera pas détourné à d'autres fins. Par exemple, la gestion de la clientèle ou encore l'enquête de satisfaction sont une finalité

Le RGPD reprend cette condition à l'article 5. Les données doivent être « *collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement*

57 Cass. crim., 1er juillet 1937, Affaire des stérilisés de Bordeaux : une stérilisation à visée contraceptive n'est pas une nécessité médicale et est donc illicite.

58 Cass. civ., 1re, 28 janvier 2010, n° 0910992

d'une manière incompatible avec ces finalités ». L'article se poursuit en considérant que le traitement ultérieur à des fins archivistiques dans l'intérêt public, à des fins de recherches scientifiques ou historiques ou à des fins statistiques n'est pas en contradiction avec la finalité initiale.

Le risque de détournement des informations, notamment des données de santé, est une préoccupation de longue date. En effet, déjà en 1995, les travaux parlementaires et l'avis du CCNE n°46 condamnaient les pratiques détournées de sa finalité initiale. L'inquiétude porte sur la réutilisation des informations par des tiers tels que les assureurs ou les employeurs.

C'est au directeur de l'établissement de santé de fixer la finalité des traitements mis en place dans son établissement. Il doit mettre tout en œuvre pour assurer le respect de la finalité. L'article 8 de la loi Informatique et Libertés énumère limitativement les cas dans lesquels le traitement de donnée est admis : traitement courants ; fins de recherche médicale ; évaluation des pratiques ; poursuite de l'intérêt public ; expression du consentement exprès de la personne, sauf si interdiction d'ordre public. En cas de modification de finalité en cours de traitement, le consentement devra alors être renouvelé. Il apparaît que la finalité du traitement semble être plus strict pour les données que pour l'acte médical. Le détournement de finalité est sanctionné pénalement.

B – Le principe de proportionnalité

Selon l'article L. 1110-5 du Code de la Santé publique, les actes médicaux ne doivent pas faire courir de risques disproportionnés au patient par rapport au bénéfice escompté. Cette démarche permet d'évaluer la pertinence des actes médicaux. Aussi, un acte de soins n'est justifié que si l'acte et ses effets sont proportionnés au bénéfice qu'en tirera le patient.

Selon le CNOM, le principe de proportionnalité « *intervient selon lequel l'évolution spontanée va être équilibrée par l'intervention médicale, avec ses divers termes et ses*

diverses conséquences, probables ou possibles»[59]. Afin que l'acte ne soit pas considéré a posteriori comme disproportionné, cela suppose en amont de déterminer le soin approprié à l'état de santé du patient. Le contrôle du Conseil d'État de l'erreur manifeste d'appréciation. La proportionnalité reste un travail complexe dans des matières aussi techniques.

Les données lors de la collecte et du traitement doivent être « adéquates, pertinentes, non excessives au regard des finalités pour lesquelles elles sont collectées et de leur traitement ultérieurs ». Parmi les premières affaires, la CNIL a refusé au courant de l'année 2000 la mise en œuvre d'un projet de contrôle d'accès biométrique du personnel de l'Académie de Lille par reconnaissance des empreintes digitales. Même réponse par les juridictions judiciaires[60]. La CNIL propose des outils afin de vérifier que les mesures prises ne sont pas disproportionnés. En ce sens des « *Risk Map* » ont vu le jour[61].

Ce principe de proportionnalité vient en complément avec le nouveau principe de minimisation de la collecte des données personnelles instauré par le RGPD[62]. Le principe de « *privacy by default* » et « *privacy by design* », c'est-à-dire dès le stade de la conception d'un produit ou service, contribue au respect de cette exigence mais n'est pas suffisant.

59 Commentaires du Conseil national de l'ordre des médecins sur l'article R. 4127-40 du CSP, article 40 du Code de déontologie médicale.
60 TGI de Paris le 19 avril 2005 n° 05/00382
61 Annexe n°2
62 Art. 5 du RGPD

SECTION II – L'encadrement par des autorités spécialisées

Avant de voir leur moyens d'actions qui sont sensiblement les mêmes dans leur domaines respectifs (B), il faut avant tout bien comprendre le fonctionnement et l'organisation des ces autorités de contrôles (A).

§1 – Les autorités de contrôle

Malgré un rôle parallèlement similaire (A), des différences dans l'organisation et le fonctionnement subsistent (B).

A – La création et leur rôle

D'une part, la Haute Autorité de santé (HAS) est une autorité publique indépendante (API) à caractère scientifique, créée par la loi du 13 août 2004 relative à l'Assurance maladie. La HAS envisage ainsi la santé dans sa globalité. D'autre part, la CNIL, créée en 1978 par la loi Informatique et Libertés, est une autorité administrative indépendante (AAI). C'est le régulateur des données personnelles.

A noter, une API est un statut juridique particulier à l'intérieure des AAI. Les AAI ne sont pas soumises à l'autorité hiérarchique d'un ministre. Pour autant, elles disposent de pouvoirs par délégation de l'État. Les deux autorités indépendantes ont plusieurs missions.

La HAS a un collège pluridisciplinaire composé de 7 membres. Le président de la république nomme par décret son président La CNIL a un collège pluridisciplinaire de 18 membres. Sa formation restreinte est composée de 5 membres.

La HAS et la CNIL ont un rôle de conseils et d'informations. Ils informent les professionnels et particuliers sur leur domaines respectifs. Ils donnent des outils afin d'adapter les pratiques et les tenir au courant des nouvelles réglementations. Ils ont également des axes de sensibilisation et de formation.

Ils donnent des avis et des décisions sur divers thématiques. Ils ont une forte portée puisque ce sont des AAI spécialisées. En ce sens, on peut notamment citer l'avis défavorable de la CNIL en 1981 sur le fichier « *GAMIN* » qui prévoyait le traitement automatisé des certificats de santé d'enfants[63].

De même, ils ont un rôle de contrôle de la conformité des textes en vigueur. Cela se concrétise par divers contrôles (ex : sur place, sur pièces etc..). Les deux organismes participent donc à l'obligation de sécurité. La HAS contrôle notamment des indicateurs de qualité et de sécurité des soins (IQSS). Ce sont aux établissements de santé de les communiquer annuellement. La CNIL quant à elle va s'assurer du respect de la réglementation sur la sécurisation des données. De plus, des procédures d'accréditations et de certifications ont été mises en place par les deux autorités.

B – Leurs différences

Il faut avoir conscience que la CNIL à un rôle plus spécifique que la HAS. Le champ de la HAS est donc plus large. En ce sens, la HAS à un plus grand éventail d'évaluations et avis. Elle évalue les médicaments, les dispositifs médicaux, les actes professionnels et fait également une évaluation médico-économique. De même, d'autres acteurs ont un rôle prépondérant dans le domaine des données tel que l'Agence nationale de la sécurité des systèmes d'information (ANSSI).

Une autre différence importante tient dans le pouvoir de sanction que détient la CNIL. A l'issue des contrôles de conformité, et d'une procédure contradictoire, la CNIL peut décider d'une sanction pécuniaire d'un montant maximal de 3 millions d'euros. Le montant des amendes est perçu par le Trésor Public et non par la CNIL. Elle peut également prononcer une injonction de cesser le traitement, un retrait de l'autorisation, ou encore en cas d'atteinte grave et immédiate aux droits et libertés, ordonner toute mesure nécessaire via la procédure de référé. Il peut également dénoncer au Procureur de la République les infractions à la législation dont il a connaissance.

63 Délibération n° 81-74 du 16 juin 1981 portant décision et avis relatifs à un traitement d'informations nominatives concernant le traitement automatisé des certificats de santé dans les services de la protection maternelle et infantile (annexe 10 au rapport d'activité de la CNIL pour 1980-1981).

De plus, il y a dans les établissements publics l'existence d'un correspondant CNIL dénommé le correspondant « Informatique et Libertés » (CIL). Avec le RGPD, le CIL a été remplacé par le DPO (« Data Protection Officer » « délégué à la protection des données »). Il fait le lien avec la CNIL et est un acteur central de la conformité. Il a pour mission de veiller à la sécurité juridique et informatique de son organisme. L'article 37 du RGPD expose les conditions d'un telle désignation.

Enfin, la CNIL à un rôle de « *Guichet unique* ». En cas d'une difficulté en lien avec la collecte ou le traitement de données, il est possible de s'adresser directement à la CNIL. Des plaintes peuvent même être formulées en ligne[64]. Les plaintes ne cessent d'ailleurs d'augmenter[65]. La CNIL va alors classer ou rejeter la plainte. Dans ce cadre, un recours est évidemment possible contre sa décision. Ce recours ne sera pas suspensif. Un référé-liberté peut également être possible si les conditions d'urgence et d'atteinte manifestement illégitime à une liberté fondamentale sont remplies.

§2 – Les moyens

Les autorités concernées utilisent des normes de soft law pour encadrer les pratiques (A). Elles sont également en charge des procédures de certifications, qui ont remplacé les accréditations (B).

A – L'utilisation de normes de soft law pour encadrer les pratiques

Un texte est dit de « *soft law* » quand il ne pose pas d'obligation juridique mais qu'il conseille ou recommande un comportement. C'est un texte de droit non contraignant, du droit souple. Il peut faire l'objet d'interprétation, notamment par le juge. Ainsi, une norme de soft law peut devenir contraignante si le juge en décide ainsi. Le développement de la soft law a parfois été critiqué notamment par ceux qui ont une vision du droit proche de celle de Jean-Jacques ROUSSEAU[66]. On retrouve de nombreuses sources de soft law

64 https://www.cnil.fr/fr/plaintes

65 https://www.data.gouv.fr/fr/datasets/plaintes-recues-par-la-cnil/

66 Selon la vision de Jean-Jacques Rousseau, il faut nécessairement que le droit pose des obligations claires, que ce soir de la "hard law".

tant au niveau médical mais aussi au niveau des traitements de données et sécurisation.

La HAS a de nombreuses normes non juridiquement contraignantes : avis, rapports d'expertises, recommandations de bonnes pratique (RPB), guides, protocoles… Les RPB ont un statut particulier, ce sont des recommandations aux professionnels de santé de prendre en charge les pathologies d'une certaine manière. Pour celles-ci, le CE a déjà admis la recevabilité d'un recours pour excès de pouvoir (REP). Par conséquent, il admet que c'est un acte qui fait grief, qui modifie l'ordonnancement juridique[67].

La CNIL a elle aussi de nombreux outils de soft law : normes ISO, les référentiels et guides de la politique générale de sécurité des systèmes d'informations de santé (PGSSI-S), cadre national d'interopérabilité des systèmes d'information de santé (CI-SIS), des documents d'information et d'aide...

La CNIL utilisait souvent des « *labels* ». Par exemple, le Programme Hôpital Numérique comprend un processus de labellisation des logiciels. On retrouvait également des procédés de labels pour les normes d'interopérabilité. Pour ces dernières, elles peuvent désormais être rendues opposables[68]. En pratique, aucune ne l'est pour le moment à défaut de la création d'un calendrier d'opposabilité[69]. Cependant, depuis l'entrée en vigueur du RGPD, il n'y a plus de délivrance de labels.

Dans les deux cas, les matières sont adaptées au développement de la soft law car ce sont des sujets techniques. En effet, les règles classiques sont parfois trop lourdes pour des situations inédites. Ainsi, le droit souple permet d'orienter les comportements sans créer d'obligations pour les professionnels. Pour autant, on voit bien que le suivi de RBP est pris en compte lors de litiges afin de s'assurer du bon comportement du professionnel.

B – Du passage de l'accréditation à la certification

La norme ISO/CEI 17000 définit l'accréditation comme une « *attestation délivrée par une*

67 CE, 27 avril 2011, Association pour une formation médicale indépendante, n° 334396
68 Depuis la loi 2016, les normes d'interopérabilité peuvent être rendues opposables par arrêté ministériel
69 Rapport annuel de la Cour des Comptes de 2018

tierce partie, ayant rapport à un organisme d'évaluation de la conformité, constituant une reconnaissance formelle de la compétence de ce dernier à réaliser des activités spécifiques d'évaluation de la conformité »[70]. Nombreuses sont les accréditations qui se sont vues transformées en procédures de certification. La certification est quant à elle « *l'attestation réalisée par une tierce partie relative à des produits, des processus, des systèmes ou des personnes* »[71].

A partir de 1999, sous la responsabilité de l'ANAES (Agence nationale d'accréditation et d'évaluation en santé) une procédure d'accréditation pour les établissements de santé publics ou privés est instaurée. Depuis 2004, sous l'égide de la HAS, elle a évolué en une certification des établissements de santé. Cette certification est une procédure d'évaluation externe des établissements de santé[72]. Celle-ci est effectuée par des professionnels mandatés. Ils évaluent la qualité et la sécurité des soins des établissements de santé. La certification est valide pour une durée qui varie entre 4 à 6 ans en fonction des comptes rendu.

Des procédures d'accréditation n'ont pas disparues. Ainsi, celle des médecins est toujours d'actualité. Cette démarche, à l'inverse de la certification de l'établissement, est volontariste. On retrouve ce dispositif à l'article L.1111-8 du CSP. Après inscription, l'équipe doit réaliser chaque année un bilan à leur organisme agréé. Un expert examinera ce bilan et portera une appréciation externe tant sur le fonctionnement de l'équipe que sur l'implication individuelle de chacun des membres de l'équipe. La HAS délivre le cas échéant une attestation et des certificats individuels d'accréditation. De même, elle délivre également l'agrément aux bases de données pour les médicaments. C'est une de ces actions de la HAS dans la procédure de certification des systèmes d'aide à la prescription, à la décision et à la dispensation de médicaments.

La CNIL est également concernée par le passage de l'accréditation à la certification. Les hébergeurs de santé étaient initialement sous une procédure d'autorisation préalable depuis 2002. Désormais, les hébergeurs de données de santé sur support numérique

70 Site web du Comité français d'accréditation (COFRAC)
71 Prec. Cit. n°70
72 Art. L6113-4 du CSP

doivent être certifiés. En effet, l'article L.1111-8 du CSP dispose aujourd'hui que « *toute personne physique ou morale qui héberge des données de santé à caractère personnel recueillies à l'occasion d'activités de prévention, de diagnostic, de soins ou de suivi médico-social pour le compte de personnes physiques ou morales à l'origine de la production ou du recueil de ces données ou pour le compte du patient lui-même, doit être agréée ou certifiée à cet effet* ». Des référentiels de certification sont mis en place par la CNIL. La certification est valide pour une durée de trois ans.

Est-ce qu'une procédure est mis en place pour des objets connectés, des applications de santé ou logiciels ? S'ils rentrent dans la qualification dispositifs médicaux (DM)[73], il feront l'objet d'une surveillance par la Commission Nationale d'Évaluation des Dispositifs Médicaux et des Technologies de Santé (CNEDiMTS). Il existe un référentiel des bonnes pratiques sur les applications et les objets connectés en santé[74]. Pour autant, il n'y a pas encore de procédés d'accréditation ou de certification.

73 Voir la définition du dispositif médical à l'article L5211-1du CSP

74 Référentiel de bonnes pratiques sur lesapplications et les objets connectés en santé (Mobile Health ou mHealth) Octobre 2016.

PARTIE II – Des différences croissantes remettant en cause la continuité ?

Comme l'introduit Monsieur Guy BRAIBANT en 1998 dans son rapport « *Données personnelles et société de l'information* », « l*es progrès intervenus dans le domaine informatique depuis vingt ans ont bouleversé les enjeux de la protection des données à caractère personnel* » [75].

Le régime de protection des données avait pour ambition de s'afficher dans la continuité des droits de la personne. Évidemment, un calquage strict n'était pas possible. Bien que certaines assimilations au corps peuvent être faite, la proximité des liens entre la personne et ses informations n'est pas toujours évidente.

Au fil des évolutions législatives, des différences se sont accentuées. L'influence originale s'est peu à peu dissipée afin d'adapter la réglementation aux nouveaux enjeux tel que le développement des nouvelles technologies et nouvelles pratiques. De multiples facteurs en sont la cause. Que ce soit la dématérialisation des données, la volonté d'ouverture des données ou encore la progression de l'intelligence artificielle, tous ces nouveaux paramètres ont dû être pris en compte afin d'améliorer la protection des données de santé.

Ainsi, il faut analyser les particularités des données de santé qui empêche une continuité forte (CHAPITRE I). Ces évolutions posent la question suivante : quelle protection dans l'avenir pour les données de santé ? (CHAPITRE II)

75 "Donnée personnelles et société de l'information" Rapport au Premier Ministre sur la transposition en droit français de la directive n°95/46 le 3 mars 1998

CHAPITRE I – Des particularités propres aux données

Les réglementations autour des données ont toujours fait l'objet de critiques. Certains considéraient même, comme Caroline ZORN-MACREZ l'écrit, que la « réglementation [est] irréaliste relative à la confidentialité des données»[76] .

Le cadre juridique des données de santé est encore à ces prémices et certains aspects pré-établis on pu être remis en cause dans le débat public. En ce sens la question de la propriété des données ne cesse d'être un sujet débattu (SECTION I).

De plus, les données de santé ne sont plus les mêmes qu'auparavant. L'ère du numérique a bousculé les schémas juridiques traditionnels. Aujourd'hui, chaque la dématérialisation des données suppose d'adapter avec une certaine souplesse les canons juridiques sans pour autant limiter les droits et libertés fondamentales (SECTION II).

76 "Chronique martienne" des données de santé numérisées. Brèves observations sur une réglementation surréaliste, Caroline ZORN-MACREZ, Revue droit & santé n°36 page 331 à 342

SECTION I – La question de la propriété des données

Pour le secrétaire d'État chargé du numérique, Mounir MAHJOUBI, la question ne se pose pas. « J*e suis contre toute propriété et vente des données personnelles. Ce que je veux, c'est la maîtrise sur ces données* »[77]. La question de la propriété des données ne cesse de revenir dans le débat national suite à certains scandales comme Google Analytica.

Les données ont une valeur économique. Leur valeur en Europe pourrait atteindre 1 000 milliards d'euros en 2020 selon le Boston Consulting Group.[78]. Pour autant, les données sont juridiquement considérées comme des « *res nullis* ». Parallèlement au principe d'inviolabilité du corps humain, les données sont considérées comme étant de nature extra-patrimonial.

Ainsi, bien que le principe soit la non patrimonialité du corps et des données (§1), les évolutions récentes vont vers la notion d'auto-détermination informationnelle (§2).

§1 – La non patrimonialité

Bien que le principe de patrimonialité semble généralement très solide concernant le corps (A), la question est bien plus discutée concernant les données personnelles (B).

A – Le principe de non patrimonialité

Qu'est-ce que la propriété ? Selon l'article 544 du Code Civil, « *la propriété est le droit de jouir et disposer des choses de la manière la plus absolue, pourvu qu'on n'en fasse pas un usage prohibé par les lois ou par les règlements* ». Ainsi, le titulaire dispose de l'usus (droit d'usage), du fructus (droits de percevoir les fruits), et de l'abusus (doit de disposer de la chose)[79]. Pour autant, le corps et les données de santé ne peuvent faire l'objet d'une telle propriété. Ils sont des droits subjectifs extra-patrimoniaux.

77 http://www.lefigaro.fr/secteur/high-tech/2018/03/13/32001-20180313ARTFIG00213-mounir-mahjoubi-je-suis-contre-toute-propriete-et-vente-des-donnees-personnelles.php
78 'The Value of our digital identity',Boston Consulting Group and Liberty Global, novembre 2012
79 Art. 544 du Code Civil

Le principe de non patrimonialité du corps se trouve à l'article 16-1 alinéa 3 du même Code « *le corps humain, ses éléments et ses produits ne peuvent faire l'objet d'un droit patrimonial* ». L'article 16-5 précise que les conventions dans ce sens sont nulles. De même, le prélèvement d'organes ou l'expérimentation ne peut pas être rémunérées[80]. Cette non patrimonialité s'explique par le principe d'indisponibilité du corps humain. Ce principe a été consacré par la Cour de Cassation[81]. La conjonction de ces deux principes empêchent notamment la vente d'éléments du corps humain ou la gestation pour autrui.

Certains auteurs estiment qu'il y a en pratique disponibilité du corps humain, ou tout du moins un assouplissement au principe, à cause des règles de gratuité et d'anonymat permettant notamment le don d'organe ou l'essai médical. Ces « *formes de disponibilités* » sur les éléments du corps humain est restreint et très encadré. Cependant, dans les deux cas, une indemnisation des frais engagés peut être envisagé.

Le principe de non patrimonialité des données de santé se retrouve quant à lui à l'article L.1111-8 du CSP. « *Tout acte de cession à titre onéreux de données de santé identifiantes directement ou indirectement, y compris avec l'accord de la personne concernée, est interdit sous peine des sanctions prévues à l'article 226-21 du code pénal* ». Ce principe rend impossible d'être propriétaire de ses données au sens de l'article 544 du Code Civil. Certains auteurs considèrent qu'un tel rapport de propriété envers les données est inenvisageable car la réglementation serait trop complexe[82]. En ce sens, comme le CNNUM l'évoquait, il est difficile de déterminer les régimes de propriété et leurs bénéficiaires[83].

Finalement, les données seraient comme un élément de la personnalité de l'homme. Le droit à la protection des données personnelles pourrait alors s'inscrire dans les droits de la personnalité a l'instar du droit à l'intégrité physique, au respect de la vie privée, du droit à l'honneur etc. Ce sont des droits que le législateur considère comme tellement important qu'il est nécessaire de les protéger.

80 Art. 15-6 du Code civil

81 Cass., ass., plén., 13 mai 1991 n°9020105

82 Voir "Propriété intellectuelle et droit commun" de N. MALLET-POUJOL, A. ROBIN, J-M BRUGUIERE, Presses Universitaires d'Aix-Marseille, 2007, p.400

83 Avis CNNUM n°1059 "Sur les données non personnelles"

B – Un principe plus discuté pour les données

La non-patrimonialité, et à fortiori l'indisponibilité, du corps humain est un principe qui a connu des controverses. Certains ont pu critiquer le manque de cohérence dans la réglementation autour de ce principe[84]. Par exemple, a été légalisée la pratique de la procréation médicalement assistée ou le suicide. Pour autant, la gestation pour autrui est toujours interdite. Dans les premiers, on est dans une logique de « *self property* » a l'image de la vision de LOCKE[85]. Désormais, ce principe fait l'objet d'un consensus relativement stable.

Ce n'est pas le cas pour les données. Le principe de patrimonialité des données étaient déjà discuté depuis les années 80, avec le slogan « Information wants to be free »[86]. Le débat s'est amplifié sur le sujet suite aux différents scandales de fuites d'informations. Cela s'explique car la donnée est devenue un enjeu contemporain, face à la société qui a évolué en une société d'informations. De fait, il y a eu une démocratisation des données personnelles tant par les nouvelles technologies que le comportement des utilisateurs. Les GAFA[87] ont su rapidement reconnaître cette conjoncture sur les données non personnelles. Ils ont gardé cette logique et font une assimilation entre donnée de santé et donnée commerciale.

La donnée de santé peut-elle être commerciale ? La donnée bien que non-patrimoniale a une valeur. C'est un « *un bien en soi* » comme le souligne Pierre CATALA[88] . Des auteurs considèrent que c'est un bien qui est juridiquement qualifiable de « *bien meuble incorporel* »[89]. De ce fait un droit de propriété à l'avenir pourrait émerger. Les États-Unis d'Amérique ont cette vision commerciale des données. En principe, les entreprises sont libres d'exploiter des données pour autant que les entreprises ne commettent pas de « *pratique déloyale* ».

84 Dans ce sens, voir "La vie, la mort, l'Etat : Le débat bioéthique" de Ruwen OGIEN, 2009, Grasset.
85 "Second Treatise of Governement" de John LOCKE, 1690
86 Formule célèbre de Stewart BRAND lors de la première Conférence des hackers de 1984
87 Le terme "GAFA" désigne les quatre grandes firmes américaines Google, Apple, Facebook, Amazon
88 "Ebauche d'une théorie juridique de l'information" de P. CATALA, 1984
89 "Etre propriétaire de ses données personnelles : peut-on recourir au régime traditionnel de propriété ?" F. MATTATIA et M. YAÏCHE, Revue Lamy de droit immatériel, 2015/114, p 60-63

Il y aurait des avantages d'une patrimonialisation des données de santé. Cela permettrai de légitimer la contractualisation de l'usage des données, de les monétiser. Pour autant, cela engendrerai des risques non négligeables. Si on part du principe que les données font parties de la personnalité de l'individu, juridiquement posséder nos données, ce serait mettre in fine à mal le principe d'indisponibilité du corps humain.

A noter que s'est également posé la question de la propriété du dossier médical. Selon Laora TILMAN, il n'existe pas de « *propriétaire* » du dossier médical[90]. En effet, l'auteur souligne que le patient à un pouvoir de contrôle et d'accès, l'établissement est responsable de la sécurité.

Il y a eu le choix d'assouplissements en France tout en maintenant le principe de non patrimonialité. Le dernier assouplissement suit le mouvement européen dans la consécration de l'autodétermination informationnelle. Bien que cette notion ravive le débat autour de la propriété des données, celle-ci ne confère pas un tel droit.

§2 – L'autodétermination informationnelle

La réglementation française va dans le sens d'une démocratisation de l'autodétermination informationnelle (A). Cette notion à une portée juridique inédite pour les particuliers (B).

A – La notion d'autodétermination informationnelle

La notion de d'autodétermination informationnelle est d'origine allemande. Elle est née d'une décision tribunal fédéral d'Allemagne datant de 1983[91]. Consciente du développement des nouvelles formes de technologies d'info / communication, le Tribunal a fait œuvre prétorienne dans le domaine. Selon sa conception, c'est « le pouvoir de l'individu de décider lui-même, sur base du concept d'autodétermination, quand et dans quelle mesure une information relevant de sa vie privée peut être communiquée à autrui ». La Commission européenne a été sensible à l'essor de l'auto-détermination

90 "La délicate question de la propriété des données de santé." L. TILMAN, Revue générale de droit médical, n°53, décembre 2014

91 Tribunal fédéral d'Allemagne, 15 décembre 1983

informationnelle. Elle avait même en 2012 le slogan suivant « *Take control of your persona! Data* » (« Prend contrôle de tes données personnelles »). En France, le Conseil d'État a eu un rôle moteur dans la consécration de la notion d'autodétermination informationnelle. En effet, il ne voulait pas établir de manière prétorienne un réel droit de propriété[92]. Ainsi, un compromis a été trouvé avec la notion d'autodétermination informationnelle. Il proposait ainsi de renforcer la place de l'individu pour « *lui permettre de décider de la communication et de l'utilisation de ses données à caractère personnel* »[93]. La loi du 7 octobre 2016 l'introduit. L'article premier dispose que « l'individu doit conserver la libre disposition de ses données ».

En somme, le principe d'autodétermination consacre une certaine maîtrise par l'individu de ses données personnelles. Cela permet à l'individu de choisir qui utilise quelles informations et pour quelle finalité. Finalement on dépasse les principes clés de la Loi Informatique et Libertés qui sont les droits d'information, d'accès, de rectification et d'opposition. On va au-delà par l'introduction de nouveaux instruments juridiques.

Du point de vue de l'individu, cela se traduit par le renforcement de mécanismes juridiques traditionnels tel que le consentement mais également de nouveaux droits comme la portabilité des données. Du point de vue des tiers, ils vont devoir se soumettre à de nouvelles obligations de transparence. Par exemple, améliorer le pouvoir de contrôle du particulier par les outils tel que le « *privacy enhancing technologies* » ou le « *privacy by design* ». Ce n'est donc pas un droit de propriété, cependant le patient dispose d'un certain contrôle sur ses données.

Cela suppose que l'individu, et donc le patient, soit en mesure d'exercer ces prérogatives. Il faudra l'éduquer sur l'utilisation des données, sur l'importance de leur circulation, les tiers impliqués tels que les plateformes, les hébergeurs ou éditeurs etc. Cependant, le choix d'un compromis via l'autodétermination informationnelle récente fait naître des risques. Cela peut entraver l'innovation et ne pas assurer une protection suffisante si les prérogatives offertes ne sont pas utilisées pour diverses raisons.

92 Rapport numérique et droit fondamentaux 2014 : "la reconnaissance du droit de propriété de l'individu sur ses données pose de sérieuses difficultés juridiques pour les pouvoirs publics"

93 Prec. Cité. n°92

Il est souhaitable de s'interroger sur la viabilité dans le temps de ce régime. Faut-il souhaiter que ce développement soit une politique vouée à la transition pour aller jusqu'à un régime de propriété ? Une politique « *des petits pas* » . Quoi qu'il en soit, son développement change la vision des données personnelles. Cela va probablement de facto faire prendre conscience aux particuliers le consumérisme existant autour de l'information, notamment autour de l'information médicale.

B – La portée juridique

L'autodétermination informationnelle se décline en plusieurs droits. On y retrouve le droit d'information, d'accès, de rectification, d'opposition, le droit à la transparence de la collecte, le droit de ne pas exporter ses données, le droit à la sécurité des données, le droit à l'anonymat, le droit à l'oubli, le droit à la mort numérique etc. La valeur juridique de l'autodétermination est législative. Ces droits peuvent être limités par les mécanismes classiques de base légale, d'intérêt public ou encore de proportionnalité. Tous ces droits seront in fine des obligations pour l'organisme ou organisation. Finalement, la réunion de ces droits permet de considérer que la condition de « l'abusus » du droit de priorité est remplie.

Un des nouveau droit important en lien avec l'autodétermination informationnelle est la portabilité des données. Il est défini à l'article L. 224-42-1 du Code de la consommation. : « *Le consommateur dispose en toutes circonstances d'un droit de récupération de l'ensemble de ses données ». Les données doivent être récupérables par le cyber-citoyen dans un standard ouvert qui doit être réutilisable et exploitable par un autre système de traitement automatisé* ». Une interopérabilité est alors nécessaire entre les différents systèmes d'informations de santé, c'est-à-dire qu'ils aient une configuration telle que les systèmes puissent interagir entre eux.

Certains auteurs sont sceptiques quant au développement de la notion d'autodétermination informationelle. Par exemple, selon Alex FLUECKIGER, professeur de droit, plusieurs critiques peuvent être formulées[94]. Il considère que l'auto-détermination

94 "L'autodétermination en matière de données personnelles : un droit (plus si) fondamental à l'ère digitale ou un nouveau droit de propriété ?" de A. FLUECKIGER, Pratique juridique actuelle, 2013, vol. 22, n° 6,

informationnelle met en danger des libertés de communication, que son contenu est lacunaire ou encore que finalement, dans la pratique, il y a une perte de la maîtrise des données personnelles.

p. 837-864

SECTION II – La dématérialisation des données

Les deux régimes ne peuvent être en tout point similaire. En effet, l'objet de la réglementation reste différent et l'évolution rapide des nouvelles technologies met en lumière la nécessaire adaptation du régime des données personnelles.

L'informatisation du système de santé à obliger le renouvellement de nombreuses règles juridiques (§1). De plus, des innovations dites disruptives ont ébranlé le système en place, mettant en lumière des vides juridiques (§2).

§1 – Du matériel à l'immatériel : changement de paradigme

La dématérialisation est l'une des principales limites au rapprochement des deux systèmes juridiques (A). Cela se concrétise d'autant plus avec l'essor du big data en santé (B).

A – Une des principales limites du rapprochement des deux systèmes juridiques

Le corps et la donnée étant deux entités différentes, il ne peut y avoir qu'influence entre eux. Ils ne peuvent pas suivre le même régime puisque le contexte n'est pas exactement le même. Des spécificités sont à prendre en compte telles que la dématérialisation des données.

Puisque notre société est devenue très connectée, il devient compliqué de protéger la dignité de chacun. Il existe désormais une captation automatique des données, mêmes celles de santé. Comme le disait Jérôme BERANGER en 2015, « *la médecine traditionnelle d'Hippocrate a laissé place à la médecine connectée et mesurée d'e-ppocr@te.* ». L'informatisation du système de santé a en effet crée de nouvelles problématiques que le droit sur la protection du corps ou la protection des données sur papier n'avaient pas à connaître. Nombreuses informations concernant la santé peuvent faire l'objet d'une collecte, notamment avec l'accroissement des objets connectés tel que les montres, les pèses personnes ou tout simplement les applications de santé sur

smartphone. De même, l'hôpital est devenu une mine d'informations avec l'imagerie, le diagnostic, les outils thérapeutiques, les données de condition physique, les outils de la pratique médicale, les données administratives[95]…

Le développement des données de santé est exponentiel. Aujourd'hui se développe également le corps connecté. Il existe désormais des médicaments connectés, des implants connectés (implantation de puces, identifications biométriques informatisées etc.). Sans parler d'un possible piratage, ces données touchent à l'intimité de la personne et sont récoltées en continu.

Les informations étaient dans un dossier papier, stocké dans un endroit déterminé et sécurisé en conséquence. Ce support était d'une certaine manière plus sécurisée. Les données numériques sont accessibles en tout lieu et à toute heure par les personnes autorisées. Cependant, il existe un risque du piratage. La possibilité d'intrusions malveillantes est inhérente au numérique, de même que des pannes, vols, erreurs fatales virus etc. Les systèmes informatiques ne peuvent pas être totalement sécurisés malgré des moyens de protections qui ne cessent de s'adapter tel que des pare-feu ou anti-virus. A l'instar des actes médicaux, il n'y a pas non plus de risque 0 pour la sécurité informatique.

Malgré cette nouvelle donne, en 2016, 88 % des français ne voulaient pas que leurs données personnelles soient exploitées[96]. Il est évident que la dématérialisation des données favorise certains risque tel que les interconnexions de données ou les collectes de masses. Cette réalité a éclaté avec l'affaire SNOWDEN. Des gardes fous sont mis en place pour éviter ce genre de pratique au nom de la protection de la vie privée. En effet, les pratiques de surveillance de masse peuvent faire l'objet d'un contrôle par différentes juridictions. En ce sens, la CEDH a déjà eu l'occasion d'invalider le process et de condamner des pays pour leur système de surveillance[97].

95 "Hôpital public et données personnelles des patients" de F. EON, RDSS "Hôpital public au début du XXI" siècle", 2015, p 85

96 Baromètre Adblocks IAB France/ Ipsos, Novembre 2016, http://www.iabfrance.com/content/presentation-de-la-v2-de-letude-ipsos-realisee-pour-liab-france-sur-les-adblocks.

97 En ce sens, voir CEDH, 4 décembre 2015, Roman Zakhaov c/ Russie ou encore CEDH, 13 janvier 2016, Haazs & Szabo c/ Hongrie.

B – Le big data en santé

Le big data est défini par l'Union européenne comme « de gros volumes de différents types de données produites à haute vitesse à partir d'un grand nombre de différents types de sources »[98]. Le big data est souvent résumé par trois expressions : volume, variété des données et variétés des modes de collectes. Il suppose le traitement de données de masse. Pour autant, il faut que les données de masses soient exploitées de manière effective afin d'en tirer un intérêt. L'agrégation simple de données n'a en soi pas d'utilité.

Le big data concerne de nombreuses données telles que les déplacements, achats en ligne, pages web consultés, centres d'intérêts, conduites à risque etc. Il permet à terme d'anticiper les comportements possibles de l'individu. Par exemple, c'est le principe de la carte de fidélité. Également il améliore les connaissances d'un contexte pour optimiser des choix stratégiques. Dans le milieu de la santé, le big data peut permettre de savoir en temps réel la durée d'une intervention chirurgicale, de prédire les influences aux urgences, de valoriser l'hospitalisation ambulatoire, etc..

Le big data est surtout connu pour alimenter l'informatique cognitive autrement connu sous le nom « *machine learning* ». En se basant sur le produit du big data, elle permet d'effectuer des prédictions à partir de bases de données. Dans la santé, ces utilisations ce développent.

Selon le rapport de Global Big Data in Healthcare Market-Analysis and Forecast 2017-2025, le marché du Big Data spécifiquement dans le secteur de la santé représentait 14,25 milliards de dollars en 2017 avec une prédiction pour 2025 à 68,75 milliards de dollars.

Le big data implique une rupture de continuité avec le corps. Comme Monsieur le Pr. LE COZ le précise « *dématérialisé, notre corps se réduit à un gisement inépuisable de données de santé à convoquer, identifier, analyser et enregistrer. Le téléchargement de*

98 Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions, "Vers une économie de la donnée prospère" COM/2014/0442

l'humain est infini »[99]. Le prisme n'est plus le même, la personne tend à s'effacer derrière la multitude de données. Cette logique s'éloigne de la logique de protection de la personne. L'identité d'une personne ne se résume pas à ces données comme il ne se résume pas à l'addition d'atomes.

Quelle place pour l'individualité ? Il ne faut pas que l'individu se résume à des capteurs de données. Une réflexion éthique doit toujours rester en ligne de mire. Est-il nécessaire d'une certification éthique des processus qui touchent au big data ? Cela suppose de se requestionner sur les valeurs individuelles et collectives. De même, il ne faut pas tomber dans ce que ROUVROY et BERNS appellent « *la gouvernementalité algorithmique* »[100].

§2 – Le cas spécifique des innovations disruptives

Les innovations « dite » disruptives en santé (A) viennent remettre en cause certains principes juridiques traditionnels (B).

A – La notion "d'innovation disruptive" en santé

La notion d'innovation disruptive est apparue dans les années 1990 sous la plume de C. CHRISTENSEN, Professeur à Harvard[101]. Pour lui, « ne sont disruptifs que les nouveaux entrants qui abordent le marché par le bas, et se servent des nouvelles technologies pour proposer des produits ou services moins chers »[102]. Finalement, c'est l'accès simplifié pour la majorité à des produits et services qui étaient difficilement accessibles jusqu'alors. Avec la révolution numérique, nombreuses sont in fine des innovations disruptives. Exemples : Ordinateurs, Iphone, Amazon, Netflix etc.. Pour autant, il ne faut pas nécessairement une technologie impressionnante pour que le produit ou service soit dit « disruptif ».

Parallèlement, le système de santé a été largement modifié par le développement des

99 "L'hébergement électronique des données de santé : vers la fin du secret médical ?" P. LE COZ, Tout dire ? Transparence ou secret, Presses Universitaires de France « Hors collection », 2012, p 17-25

100 Voir "Gouvernementalité algorithmique et perspectives d'émancipation" de A. ROUVROY et T. BERNS, Réseaux, La Découverte, 2013/1 n°177

101 Voir "Le dilemme de l'innovateur" de C. CHRISTENSEN,1997

102 Selon l'auteur sur son site http://www.claytonchristensen.com/key-concepts/

nouvelles technologies et ne cessent d'être un secteur prolifique aux innovations disruptives. Exemples en santé : Objets connectés, thérapie génique, nano-médecine, impression 3D d'organes, l'envoi de produits pharmaceutique à domicile[103] etc.. Finalement, cela change la pratique des équipes, des professions et le système de santé s'en retrouve ainsi impacté. La notion d'innovation disruptif à un écho particulier dans le secteur de la santé puisqu'une logique de maîtrise des coûts est sous-jacente.

Une innovation disruptive importante en santé est la télémédecine. Elle se décline sous différentes formes : télé-expertise, de télé-consultation, de télé-surveillance, de télé-assistance. Les consultations ne se font plus face à face. La relation patient-médecin s'en trouve modifiée. C'est une des solutions privilégiées pour faire face aux déserts médicaux. De même se développe les systèmes d'aide à la décision (SADM). Ils évoluent pour devenir un support à la décision thérapeutique, devient indispensable à l'exercice médical. Ces progrès améliorent la qualité de la prise en charge des patients (rapidité du diagnostic, réponse adéquat à la problématique...) Cependant, ils n'ont pas pour objectif de substituer à la responsabilité des médecins, ni à leur liberté de prescription. Enfin, il y a également le développement de l'intelligence artificielle dans le domaine de la santé. En ce sens, il existe notamment l'IA « Watson »[104].

Comment protéger les données lorsque des innovations rendent rapidement inadaptées le droit existant? Faut-il considérer que les progrès technologiques étant toujours en avance par rapport à la réglementation il est compliqué d'anticiper de telles innovations, et qu'il faut donc se résoudre à réglementer les abus à posteriori ? En tout état de cause, il est clair que ces innovations remettent parfois en cause des principes juridiques traditionnels.

B – La remise en cause de principes juridiques traditionnels

Avec l'émergence de nouvelles pratiques, de nouveaux standards, des principes juridiques classiques montrent leurs insuffisances à s'adapter. Ainsi, on retrouve un nouveau marqueur de rupture entre le régime de protection des données et le régime de

103 Start up Américaine "Capsule" https://www.capsulecares.com/
104 Voir l'IA Watson https://www.ibm.com/watson/

protection de la personne.

Par exemple, la notion même de vie privée est discutée. Peut-on vraiment considérer que la vie privée d'aujourd'hui est la même que celle d'avant les réseaux sociaux ? Les conditions d'utilisations de ces plate-formes ne cessent de s'assouplir[105]. Il est légitime de se demander ainsi s'il est possible d'assurer la même protection de la vie privée qu'avant l'émergence de ces innovations disruptives. Dans le domaine de la santé, c'est la notion de secret médical qui a dû évoluer avec des assouplissements liés au partage d'informations.

De même, la protection des données tente de pallier à la faiblesse du consentement. Celui ci n'est pas réel lorsqu'il y a autant de contrats d'adhésion non négociables. Il est donc entendable que le choix du consentement par non opposition est plus réaliste pour la protection des données. En parallèle, s'est donc développée la notion autodétermination informationnelle pour pallier.

Le principe de finalité dans le traitement des données peut également être remis en cause par l'avènement du big data. Le but du big data est bien de pouvoir utiliser des données pour des finalités diverses qui ne peuvent pas ou ne sont pas toujours prévues.

Autre exemple avec les SADM. La question de la conformité aux textes en vigueur s'est posée. En effet, l'article 69 du Code de déontologie médical dispose bien que « L'exercice de la médecine est personnel ». Tant qu'il n'y a pas dans les faits une SADM automatique sans regard par le médecin, il n'y aura pas d'atteinte aux principes déontologiques et législatifs. Quelle responsabilité en cas de dommage lié au SADM ? Il faudra alors distinguer ce qui est du fait du concepteur du SADM et ce qui est du fait du médecin.

Dernier exemple avec l'IA : les mécanismes de responsabilité actuels ne sont pas adaptés. Récemment, cette question a été d'actualité avec les voitures autonomes de Google. Il n'existe pas actuellement de régime juridique propre à l'intelligence artificielle, et aucun fondement juridique n'y apporte de réponse spécifique ». La responsabilité du fait

105 Voir l'évolution des conditions générales de Facebook sur http://owni.fr/2010/05/05/historique-de-l%E2%80%99erosion-de-la-vie-privee-sur-facebook/

des choses ne s'applique pas puisque le médecin n'a pas l'usage, la direction et le contrôle au moment du dommage. L'ingénieur quant à lui ne connaît pas l'algorithme utilisé par la machine.

De nombreuses questions similaires vont se poser avec les robots assistants, le développement de la « Gérontechnologie »[106] ou encore la démocratisation des imprimantes 3D.

106 "Aging, Well-Being, and Technology: From Quality of Life Improvement to Digital Rights Management — A French and European Perspective" de N. DEVILLIER, IEEE Communications Standards Magazine, 2017

CHAPITRE II – Quelle protection des données pour l'avenir ?

Bien que le RGPD est récemment entré en vigueur, la matière ne va de cesse d'évoluer. Ainsi, il est intéressant de s'interroger sur la direction que les prochaines révisions vont prendre.

Le système de protection de la personne est assez strict. Un renforcement de la protection des données se traduirai par une plus grande autonomie de l'individu sur le sort de ses données de santé. Il est vrai qu'il est possible de questionner la pertinence d'un renforcement de la protection des données de santé semblable à la protection de la personne (SECTION I).

Or, les dernières avancées législatives ne cessent d'assouplir certaines règles et de prôner la circulation des informations. Cette diffusion semble donc marquer un coup d'arrêt avec l'influence du droit de la personne. Entre-t-on dans une politique libérale de la protection des données de santé, vers une rupture de continuité ? (SECTION II).

SECTION I – La pertinence d'un renforcement de la protection des données de santé semblable à la protection de la personne ?

On peut dire que le système de protection de la personne est assez strict et effectif. Suites aux bouleversements récents, les formes traditionnelles ne suffisent plus. A première vue, s'il faut poursuivre dans la continuité et la cohérence entre les deux régimes, il faudra, persévérer pour que le régime de protection des données soit à un degré de sécurité efficace.

Ce renforcement a d'une part des avantages qui sont globalement reconnus (§1). Pour autant, des inconvénients doivent être mis en lumière afin de comprendre la tendance à la libéralisation des données (§2).

§1 – Les avantages d'un renforcement au nom de la continuité

Le meilleur contrôle par la personne de ses données personnelles (A) permettra de limiter les abus, les risques d'une utilisation inappropriée par les tiers (B).

A – Un meilleur contrôle par l'individu de ses données

Un renforcement des droits fondamentaux, du droit à la confidentialité, à l'intimité permettra à l'individu d'avoir un meilleur contrôle de ses données. Dans ce sens, il s'agit d'améliorer l'autonomie de la volonté qui est un critère clé dans notre société démocratique actuelle. Éthiquement, cela permettrait de remettre le patient au centre de sa prise en charge et ainsi s'éloigner d'une relation patient-hôpital désincarnée. Encadrer strictement les données de santé permettrait à l'individu de récupérer une plus grande maîtrise sur les informations le concernant. Un tel renforcement nécessitera de remettre en cause certaines avancées qui vont dans le sens de la souplesse.

Dans le cadre actuel, le patient gère ses données, à lui d'apprécier s'il faut partager ou non des données de santé. Le patient devient acteur de son identité. Il possède plus de droits effectifs. Il peut sélectionner les informations qu'il souhaite rendre visible ou non. Si

on extrapole, dans un régime de propriété, il pourrait engendrer des gains avec.

Le renforcement du cadre actuel passera par une meilleure transparence afin que les personnes aient confiance sur trois échelles différentes.

En premier lieu, une confiance dans des outils qui ne sont pas neutres. Il faut que le patient puisse exploiter lui-même ses données. Cela engendrera une plus grande utilisation des objets connectés sans avoir peur des conséquences sur les données. Par exemple, si le DMP n'a pas fonctionné c'est notamment parce que la confiance de la population n'était pas au rendez-vous. Malgré l'envie des français[107], ils restent sur la défensive car ils n'ont pas l'impression d'avoir une réelle maîtrise de l'outil. Cependant, il ne faut pas en arriver à de l'autorégulation automatique.

En deuxième lieu, une confiance dans le système de santé. « *Sans confiance des citoyens dans la protection des données confidentielles, il ne peut exister de système d'information viable »* [108]. Une telle confiance permettra une meilleure santé publique, mais aussi de sauvegarder l'exercice hospitalier. La crise de confiance sur les vaccins ou sur certains médicaments réduit la pleine effectivité de nombreux actions de préventions thérapeutiques.

En troisième et dernier lieu, une confiance dans les tiers. Un rapport plus équilibré pourrait se mettre en place entre tous les acteurs du domaine. Encadrer plus strictement les tiers tels que les GAFA à l'instar des hébergeurs sur le sujet pourrait permettre d'améliorer les rapport entre les particuliers et eux. En effet, la peur de voir des risques d'une utilisation inappropriée serait amoindrie.

B – Moins de risque d'une utilisation inappropriée par les tiers

Avec la dématérialisation des données, celles-ci sont plus facilement exploitables par des

107 "Français sur 10 prêts à être équipés pour suivre leur maladie chronique" Enquête Unicancer http://www.unicancer.fr/sites/default/files/actualite/SOUS%20EMBARGO_Odoxa%20pour%20Unicancer-oct-2017%20rapport%20complet%20avec%20synthese_VDEF-2.pdf

108 "Rapport sur la gouvernance et l'utilisation des données de santé" PL BRAS et A. LOTH, Ministère de la Santé et des Affaires sociales, 2013.

tiers. Un renforcement de la protection légale permettrait d'éviter les abus.

Les GAFA ont la capacité de regrouper les données pour mieux cibler les publicités. Ils utilisent des algorithmes afin de pouvoir analyser les comportements des clients potentiels. Le but est de pouvoir anticiper leurs besoins afin d'apporter des publicités personnalisées. Ainsi, ils sont conscients de l'apport de telles données et n'hésitent pas à faire de nombreux projets / business plan dans le domaine[109]. Sachant qu'il existe un rapport déséquilibré entre les GAFA et les particuliers, une meilleure protection permettrait un rééquilibrage dans l'utilisation des données de santé. Ainsi, il y aurait moins de data trading, ou encore moins de data brokers (courtiers en données)[110].

Le renforcement permettrait également d'éviter les procédés de surveillances de masse. Le risque de profilage, c'est-à-dire, d'être classé dans une catégorie selon différents critères, serait amoindrie tout autant. Bien que ce soit une pratique existante avant le big data, la révolution numérique a simplifié les moyens de le faire. Par exemple, la carte de fidélité dans une enseigne de grande surface va pouvoir identifier si une personne mange trop gras ou trop salé. Celle-ci risque d'être repérée et stigmatisée, voire in fine ne plus être assurée. Par ailleurs un tel programme a été développé en Chine. Un plan directeur pour la construction d'un système de crédit social (2014-2020) a été validé afin de construire un système de « réputation nationale » en utilisant les données numériques personnelles.

Il faut donc éviter une « cartographie quasi- complète de l'individu numérisé »[111] afin de limiter tant que possible toutes sortes de discriminations. En somme, cela revient à limiter les abus des mécanismes d'interopérabilité des bases de données.

§2 – Les risques si renforcement au nom de la continuité

Si on renforce la protection des données, il y a ne faut pas sous estimer les conséquences

109 ""Santé" et "Big data" : Google à l'origine d'une nouvelle ère d'encadrement des données personnelles de santé ?" A. NIETO, Revue droit & Santé n°67 p 649-650

110 "Data Brokers : A call for transparency and accountability", Federal Trade Commission FTC, 2014

111 "La gouvernance des Big data utilisées en santé, un enjeu national et international", de E. RIAL-SEBBAG, Journal International de Bioéthique 2017/3, Vol. 28, p 39-50

et les responsabilités du patient (A). Au-delà, existera un risque de surprotection de l'individualité au détriment de la collectivité (B).

A – Les conséquences et responsabilités du patient dans la « gestion de ses données »

Aujourd'hui, la responsabilité de la gestion des données n'est pas octroyée aux particuliers mais aux organisations ou sociétés qui les exploitent. Le RGPD a d'ailleurs alourdi cette responsabilité. Ce mécanisme peut finalement paraître plus sécurisant que si l'individu était lui-même responsable de ses propres données.

Afin d'avoir une gestion raisonnable, il est nécessaire qu'une éducation spécifique soit mise en place. C'est le rôle de la CNIL de promouvoir des outils de management des données personnelles. Il en existe déjà, mais c'est actuellement limité au organisations. A l'avenir, il se peut que ceux-ci soient adaptés aux personnes privées. En l'état actuel des pratiques, il y a un manque d'informations pour que les individus puissent réellement saisir la pleine portée de la responsabilité de cette gestion des données. C'est un travail à réaliser sur plusieurs années. Ainsi, porter la responsabilité sur l'individu peut paraître prématuré.

De plus, il y a un risque de rupture d'égalité. Le domaine de la gestion des données reste peu connu des citoyens. Est-ce vraiment protecteur de laisser à chacun la détermination de son niveau de protection optimal de ses données, de sa vie privée informationnelle. Cela va générer des inégalités ou les renforcer.

De même, des règles trop strictes vont entraîner un frein économique. L'exploitation des données est un stimulant pour l'économie comme le souligne Henri VERDIER[112]. La valeur informationnelle est comparée à une matière première. En effet, les organismes et les entreprises vont exploiter ces données pour améliorer leur performance soit en limitant des coûts de production soit en développant des revenus. Donc si on laisse le citoyen mettre trop de verrous protecteurs, il y a un risque d'une sous exploitation qui impactera

112 Entretien avec Henri Verdier réalisé par Pierre-Yves Baudot "Au-delà de l'ouverture des données, ce qui est en jeu, c'est l'ouverture de la décision", Informations sociales 2015/5, n° 191, p. 20-25.

négativement à plus ou moins long terme l ’économie et l’innovation.

Faut-il s’inquiéter de la responsabilité juridique du patient en cas de mauvaise gestion? Le risque est de pouvoir se refuser une prestation. Actuellement, en droit médical, même s’il ne suit pas le traitement ou les préconisations, il ne peut y avoir d'effets sur le remboursement de la prise en charge. Par exemple, le propos a été étudié pour un cas d'apnée du sommeil. Il fallait que le patient utilise à minima le dispositif pour se faire rembourser par l’Assurance Maladie. Les données d’utilisations étaient automatiquement envoyées à celle-ci. Cette pratique à fait polémique. Une délibération de la CNIL[113] a annulé l’autorisation unique suite à une annulation du CE[114]. Ce dernier ne s’est pas prononcé sur le bien-fondé mais a annulé les arrêtés pour incompétence.

Ne vaut-il pas mieux que les organismes restent responsables comme aujourd'hui ? L’absence de véritable propriétaire est peut-être finalement une garantie forte pour assurer une protection efficace des données sensibles sans rupture d’égalité trop forte. Certes, c’est une vision paternaliste comme c’était le cas dans la relation patient-médecin. Reste à savoir si cette vision s'érodera également

B – De surprotection de l'individu au détriment de la santé collective ?

Les libertés individuelles peuvent être limitées pour l’intérêt général, pour le bien commun. C’est une logique de droit public qui se retrouve dans de nombreux dispositifs légaux. En droit médical, l’obligation vaccinale reflète les limites aux libertés individuelles lorsque des enjeux de santé publique sont majeurs. Cependant, lorsque la réglementation est trop protectrice des libertés individuelles, l’intérêt général s’y trouve lésé.

Les bases de données médico-administratives permettent une meilleure surveillance sanitaire de la population[115].L'analyse de ses données engendre des décisions pour

113 Délibération n° 2014-528 du 11 décembre 2014 portant abrogation de l'autorisation unique n° 2014-046 du 30 janvier 2014 relative aux traitements de données à caractère personnel mis en œuvre par les prestataires de santé à domicile pour la téléobservance (AU-033)

114 CE, 28 novembre 2014, n°366931

115 "Les bases de données médico-administratives : un nouveau souffle pour la surveillance en la santé publique ?" de D.A. ROY et J-C DESENCLOS, Bull Epidémiol Hebd. 2013, Hors-Série

assurer le maintien de la santé/sécurité des tiers, pour améliorer les politiques de prévention, pour piloter efficacement les politiques publiques etc.. Elles ont également une utilité aux vues des préoccupations médico-économiques actuelles.

En France, la base de donnée la plus importante dans le domaine de la santé est le système national d'information interrégimes de l'Assurance Maladie (SNIIRAM). Les données sont anonymes. On y trouve des informations concernant les remboursements effectués par l'ensemble des régimes d'assurance maladie pour les soins du secteur libéral ainsi que les informations sur les séjours hospitaliers via le PMSI (Programme de médicalisation des systèmes d'information) des hôpitaux. Le SNIIRAM constitue donc une base de données majeure.

Concrètement, avec l'utilisation des données de santé, il est possible de repérer certaines pathologies, surveiller des pathologies chroniques, évaluer des actions de prévention (vaccins, dosage des marqueurs de cancer...), avoir une meilleure compréhension des déterminants de santé, renforcer la pharmacovigilance, prévenir des comportements dangereux, améliorer des différentes études d'impact.. Il y malgré tout des limites aux bases de données. Par exemple, si une maladie ne nécessite ni hospitalisation ni prise en charge en ALD, celle-ci sera difficile à repérer. En ce sens, peut être que le scandale du Médiator aurait pu être détecté plus rapidement. Ces bases de données peuvent également être croiser avec des cohortes. En ce sens, il a été analysé qu'une perte de poids d'un point d'indice de masse corporelle entraînait une baisse de tension artérielle significative. Ces données sont des outils afin que les établissements et collectivités adaptent leurs pratiques, progressent dans leur savoir faire. A l'inverse, il ne faut pas tomber dans la surprotection collective au détriment des libertés individuelles.

Au final, la surprotection de l'individu serait également préjudiciable pour les intérêts des particuliers. En effet, une multitude de réglementations sur la donnée empêcherait une certaine fluidité des parcours de soins. Il faut que la réglementation soit réaliste. Une règle trop complexe serait alors contre productive.

SECTION II – Vers une rupture de continuité ?

En dehors des souplesses ponctuelles afin de s'adapter au TIC , on retrouve une réelle philosophie d'ouverture des données (§1). Au vu de l'évolution des pratiques, quel peut être l'avenir de notre réglementation des données de santé? Quelques propositions de conciliations peuvent en découler(§2) ?

§1 – La philosophie de l'ouverture des données

L'ouverture des données a été prôné à différentes strates (A) et a débouché en France au Système National des Données de Santé (B).

A – Des textes européens et nationaux qui prône la circulation et l'ouverture des données

Alors que les politiques publiques cherchent à favoriser le renforcement des droits des particuliers sur les données, une politique d'ouverture des données dite « publiques » fait son avancée en parallèle. Ces deux visions sont loin d'être antinomiques. C'est une complémentarité. Selon Opendata France, « *L'ouverture des données est une politique publique qui développe des portails de mise à disposition de données et favorise la mobilisation et la réutilisation de données dans l'action publique* »[116]. Cette démarche s'inscrit dans le droit de la société de demander des compte à tout agent public à son administration[117].

La Commission européenne fait partie des acteurs qui ont impulsé cette ouverture des données. Une directive de 2003[118] prévoyait déjà des cas où la réutilisation des données seraient possibles. Cette directive a été revue 10 ans plus tard. Là où il y avait des autorisations, la directive de 2013[119] promeut un réel droit à la réutilisation des données

116 http://www.opendatafrance.net/ressources/

117 Art. 15 de la Déclaration des droits de l'homme et du citoyen de 1789

118 Directive européenne 2003/98/CE du 17 novembre 2003 concernant la réutilisation des informations du secteur public

119 Directive européenne 2013/37/UE du 26 juin 2013 modifiant la directive 2003/98/CE concernant la réutilisation des informations du secteur public

publiques. En France, on retrouve ce postulat dans la loi Pour une République numérique. Pour autant, cette démarche n'est pas complètement nouvelle. Il y a depuis la loi CADA de 1978[120] un droit d'accès aux documents administratifs. Celle-ci considère que les données produites ou détenues par les administrations, dans le cadre de leurs missions de service public, doivent être mises à disposition du public.

La notion de donnée publique a évolué dans une vision stricte. En 2013, une donnée publique est définie comme « *toute information produite ou reçue, dans le cadre de leur mission de service public, par l'Etat, les collectivités territoriales ainsi que par les autres personnes de droit public ou les personnes de droit privé chargées d'une telle missio*n »[121]. Avec la loi Pour une république numérique, les données publiques sont devenues des « *informations publiques* » contenues dans des « *documents communiqués ou publiés par les administrations* ». Tous les documents ne sont pas transmissibles. En principe, les dossiers tenant à la vie privée, au secret médical, au secret commercial et industriel ne ne doivent pas être communiqués. Leur diffusion est possible si les informations sont rendues anonymes avant communication.

La France s'est investie dans cette politique d'ouverture des données. Elle a signé « *l'Open Data Charter* », charte internationale qui définie les principes majeurs en la matière. La France est classée 4ème au niveau international selon « *The Global Open Data Index* »[122] en prenant compte différentes catégories[123]. Le programme est mis en place depuis 2011 à partir du site web http://www.data.gouv.fr/.

En plus d'être dans une politique de transparence de l'État et d'accroître la participation citoyenne, l'Open data permet de moderniser l'action publique et de développer l'économie nationale. Les jeux de données vont servir tant aux acteurs publics que privés. Cette politique d'ouverture s'est également étendue dans le domaine de la santé.

120 Loi n° 78-753 du 17 juillet 1978 portant diverses mesures d'amélioration des relations entre l'administration et le public et diverses dispositions d'ordre administratif, social et fiscal
121 http://www.vie-publique.fr/actualite/alaune/administration-vers-portail-acces-aux-donnees-publiques.html
122 https://index.okfn.org/place/
123 Annexe n°3

B – Le SNDS : l'open data des données de santé

L'article 47 de loi de modernisation de notre système de santé organise un open data de la santé connu sous le SNDS (Système national des données de santé). L'accès aux bases de données n'est pas complètement ouvert. Elles ne peuvent être utilisées que sous l'autorisation de la CNIL à des fins de recherches, d'études ou d'évaluations d'intérêt public. Une demande doit être déposée auprès de l'Institut National des Données de Santé (INDS)[124]. Cette procédure limitative d'ouverture des données n'est pas une spécificité française, En 2016, pas plus d'un tiers des pays dans le monde avait un open data des données de santé systématiquement ouvert.[125].

Dans le SNDS on retrouve les données du SNIIRAM. Le SNIIRAM a été créé par la loi de financement de la sécurité sociale pour 1999. On retrouve son dispositif à l'article L.161-28-1 CSS. Bien que les dispositions législatives prévoient l'anonymisation des données sensibles, le risque de ré-identification est réel. Par exemple, il a été démontré en 2014 que via les données du PMSI, 89 % des personnes pouvaient être identifiées par le mois du séjour, le code postal, l'âge, le sexe et le nom de l'établissement et que ce taux montait à 100 % en cas de deux hospitalisations dans l'année. [126]

Le SNDS a déjà fait l'objet de réutilisations. Par exemple, en médico-économique et social, les jeux de données ont fait l'objet de recherches sur la consommation de soins des bénéficiaires de la CMUC ou de l'ACS[127]. Les chercheurs ont conclu que la population étant assurée par l'ACS a une fréquence de pathologie et d'hospitalisation similaire voir supérieure à celle assurée par la CMUC et que ces deux populations ont majoritairement une nécessité de soins pour des pathologies chroniques. Autre exemple concernant les parcours et offres, les motifs de recours pour l'hospitalisation de court séjour en 2013 ont

124 Annexe n°4

125 "World Health Organization Member States and Open Health Data: An Observational Study" C. GREENBERG et S. NARANG

126 Selon P. BURNEL et F. VON LENNEP

127 "Consommations de soins des bénéficiaires de la couverture maladie universelle complémentaire (CMUC) ou de l'aide pour une complémentaire santé (ACS) en 2012", Revue d'épidémiologie et de santé publique 64 (2016) 64-78. P. TUPPIN, S. SAMSON, N. COLINOT, C. GASTALDI-MENAGER, A. FAGOT-CAMPAGNA, C. GISSOT

été analysés[128][129].

Elizabeth PISANIA et Carla ABOUZAHRB[130] illustrent parfaitement les inquiétudes quant au développement du partage des données. « *Sharing health data: good intentions are not enough* » (« *Le partage des données de santé : les bonnes intentions ne sont pas suffisantes* »). Il faut en effet que la confidentialité soit bien respectée sous peine d'un échec. En ce sens, le Royaume Uni, un des leaders de l'open data a, suite à un scandale de vente des données[131], dû abandonné son projet d'un système national des données de santé en 2016.

§2 – Propositions de conciliations

Au-delà d'un nécessaire consensus international pour assurer une protection globale et effective (A), certaines pistes peuvent déjà être explorées (B).

A – Un nécessaire consensus international

La nécessité d'un consensus international était déjà une préoccupation définie en 1978. L'article 1er de la loi Informatique et Libertés dispose en ce sens que : « *L'informatique doit être au service de chaque citoyen. Son développement doit s'opérer dans le cadre de la coopération internationale* ». Bien qu'un travail au niveau européen ait été fait avec le RGPD, les échanges d'informations ne se limitent pas aux frontières européennes. La coopération européenne n'est pas suffisante. Les données n'ont pas de frontières et les différences entre les autres pays mettent à mal les principes européens.

De plus, l'absence d'un cadre unique entrave l'innovation. Les entreprises doivent gérer différentes législations dès lors qu'un produit ou un service sera commercialisé sur le plan international. C'est un facteur de complexités puisque les sociétés doivent faire attention

128 "Hospitalisation de court séjour : quels motifs de recours en 2013?" par Marie-Claude Mouquet, Etudes & Résultats 2015 n°928

129 Annexe n°5

130 Bull World Health Organ 2010;88:462–466 | doi:10.2471/BLT.09.074393Introduction

131 https://www.telegraph.co.uk/science/2016/07/06/controversial-50-million-nhs-database-scrapped-quietly-on-same-d/.

aux éventuelles contradictions entre législations. Sachant que les GAFA investissement dans les données de santé, une harmonisation internationale devra s'établir afin de protéger au mieux le droits de la personne.

Pour autant, en pratique la mise en place sera complexe. En effet, ces notions de sécurité et de confidentialité peuvent être subjectives d'un pays à un autre. Elle ne sont pas entendues similairement à travers le monde. Les visions ne sont pas identiques. Ainsi, aux États-Unis d'Amérique, l'utilisation des données personnelles est sujet moins sensible qu'en France.

De plus, une particularité dans ce domaine est la difficulté d'avoir une vision à plus long terme. Les pratiques et les technologies en lien avec la e-santé ont toujours une longueur d'avance devant les règles juridiques. Depuis le début, les règles ont été progressivement adaptées en fonction des pratiques de terrain. Il y a une réelle difficulté à anticiper ce qui rajoute un défi supplémentaire.

L'OMS en 2012 a fait une enquête sur les « *Cadres juridiques pour la cyber-santé* »[132]. La majorité des pays du monde a adopté une législation afin de garantir les droits fondamentaux dans le domaine, celles de l'Europe sont plus développées que dans les autres Régions du monde. Certains sujets n'y sont mêmes pas abordées, comme par exemple l'accès aux données des dossiers médicaux électroniques à des fins de recherches. Pour autant, l'OMS ne semble pas se pencher sur la question d'une harmonisation internationale.

Finalement, est-ce que le RGPD, l'harmonisation la plus aboutie à ce jour, pourra avoir une portée internationale ? Il est certain que cela va harmoniser quelques pratiques en dehors même de l'Europe. Sachant que le RGPD a nécessité environs 6 ans de travail, une législation internationale demandera un investissement d'une plus longue haleine.

132 "Cadres juridiques pour la cybersanté : sur la base des résultats de la deuxième enquête mondiale sur la cybersanté", Collection de l'Observatoire mondial de la cybersanté, v. 5

B – Quelques pistes particulières

Afin d'être en adéquation avec la pratique, il faut que les législations sur les données aient une certaine souplesse avec l'émergence des nouvelles technologies. Cette souplesse n'équivaut pas à un système libéral et non protecteur. Au contraire, une souplesse est parfois nécessaire afin que les droits soient réellement effectifs.

La première piste consisterait peut être à ce que la donnée de santé soit sujette à différentes qualifications en fonction de l'utilisation. Comme le propose Emmanuelle RIAL-SEBBAG, pour elle « *la donnée ne peut être envisagée dorénavant qu'au sein d'un cycle, faisant donc évoluer sa qualification juridique (et son régime) au fil du temps* ».[133].

Faut-il faire évoluer la notion de vie privée ? La notion de vie privée entendue traditionnellement n'est pas toujours adaptée, elle peut être perçue comme « *une norme sociale anachronique »*[134]. Il est vrai que la vie privée ne peut plus être totale dans une société connectée en permanence. Pour autant, les données sensibles doivent rester sous l'égide d'une telle protection constitutionnelle. Ces constatations feront t'elles émerger une notion autonome autour de « *la vie privée médicale connectée* »[135] ?

Concernant le dossier médical partagé, afin que celui-ci puisse réellement prospérer et améliorer les prises en charge, des évolutions sont à envisager. Faut-il par exemple, comme dans d'autres états tel le Danemark, « supprimer » le consentement du patient puisque chaque citoyen détient d'office un dossier médical partagé .

Il semble également préférable de renforcer l'auto-détermination, de s'assurer et de promouvoir les droits effectifs. Il faut développer également les moyens de recours des particuliers contre les grandes entreprises. L'auto détermination informationnelle apporte finalement la souplesse nécessaire permettant de concilier différentes préoccupations. Évoluer prochainement dans un régime de propriété semble prématurée. Les questions et

133 "La gouvernance des Big data utilisées en santé, un enjeu national et international" E. RIAL-SEBBAG, Journal International de Bioéthique 2017/3 (Vol. 28), p. 39-50. DOI 10.3917/jib.283.0039

134 Selon la formule de Marc Zuckerberg, fondateur de Facebook

135 ""Santé" et "Big data" : Google à l'origine d'une nouvelle ère d'encadrement des données personnelles de santé ?" A. NIETO, Revue droit & Santé n°67 p 649-650

problématiques ne sont pas encore intégrées par la conscience collective.

Avec le développement croissant du SNDS, faut-il concevoir une responsabilité sans faute en cas de dommages liés à l'utilisation de données de santé dans l'intérêt général à l'instar des dommages liés aux vaccins ? La profusion des régimes sans faute dans le domaine de la santé sont parfois critiqués et coûteux pour les finances publiques. Pour autant, cette possibilité semble cohérente si certains critères sont développés tels que le préjudice spécial et anormal.

Les réflexions sur un régime juridique pour les IA dont celles spécifiques au domaine de la santé doivent se poursuivre. Le député Cédric VILLANI a soumis en mars 2018 un rapport dans lequel il préconise de renforcer la réglementation actuelle. En parallèle, face à l'utilisation exponentielle des IA sur le marché il faudrait mener une réflexion sur les règles de responsabilités. Laisser un tel domaine à la sagesse des juges ne procure pas une sécurité juridique suffisante.

Enfin, il serait pertinent d'une part de renouveler et moderniser les instruments de soft law supra-national et d'autre part d'envisager la préparation d'une déclaration internationale sur les données et la protection des droits fondamentaux. A ce jour, concernant les données, il n'y a qu'une déclaration internationale sur les données génétiques humaines qui date de 2003. Une harmonisation internationale pourrait alors s'inspirer des grands principes du RGPD.

CONCLUSION

La législation sur la protection des données a été influencée par celle des droits de la personne. La philosophie derrière l'élaboration des lois autour des données de santé est toujours à la recherche de la protection de la personne. Cette préoccupation se démontre que ce soit au travers de l'existence de droits fondamentaux dans son régime juridique via la primauté de la volonté de la personne ou sa vie privée qu'au travers des principes déterminants dans la prise en charge et de l'encadrement particulier.

Le régime juridique des données de santé a dû faire face à des particularités qui ne pouvaient pas être ignorées. Que ce soit la dématérialisation des données ou le débat sur la propriété des données, ces assouplissements ont été instauré afin que le régime soit cohérent et surtout efficace en pratique. Ces prémices de souplesses ont pu faire naître des inquiétudes pour l'avenir du régime et remet dans le débat des visions divergentes sur le sujet.

Au fil des modifications, les règles ont été précisées, les droits de la personne ont été renforcés. Ces évolutions assurent une meilleure sécurité juridique pour les personnes. Les libertés fondamentales arrivent à être renforcées sans pour autant que l'intérêt général subissent des conséquences.

Certaines limites de l'influence des droits de la personne sont apparues et les règles autour des données de santé ont dû s'adapter en conséquence. Il ne faut pas perdre de vue que la donnée est un enjeu de gestion des institutions et des politiques publiques[136], quel que soit le domaine. Ainsi, aux vues des enjeux contemporains, notamment des dépenses de santé publiques, la donnée ne peut pas s'enfermer sur elle-même.

Les principes moteurs restent inchangés, la philosophie cherche toujours à concilier au mieux libertés individuelles et intérêt général. Il paraît donc difficile d'afficher une réelle rupture entre les deux régimes. La législation française actuelle n'est pas ancrée dans une vision libérale du traitement et du partage des données de santé. Il y a donc toujours une

136 "Informatisation et confidentialité des données médicales" M. BRODIN, Laennec 2007/1 Pages 12-22

continuité et les perspectives proches ne contrarient pas cette affirmation. Cependant, le lien entre les deux régimes de protection n'est plus aussi évident, les convergences sont de moins en moins nombreuses.

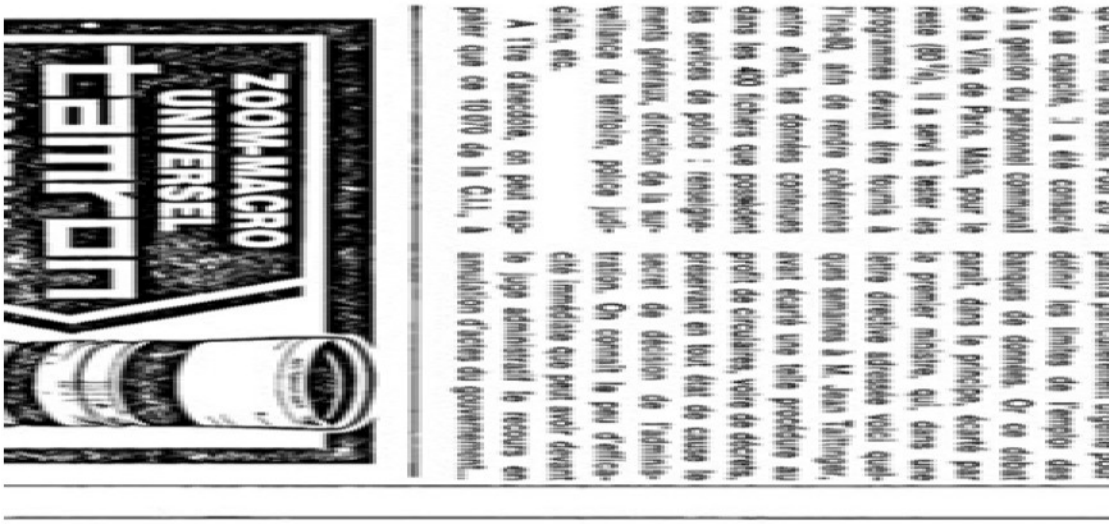
« *Par un retournement surprenant, la transparence démocratique de l'Internet […] devient la pire menace pour la liberté de l'individu* »[137]. La transparence est devenu un leitmotiv de notre société. La protection des données n'y échappe pas. Il y a une volonté d'outrepasser un régime juridique qui était opaque et conjointement, ouvrir des bases de données de santé. Pour autant, celle-ci ne doit pas affaiblir les droits et les libertés individuelles comme le souligne Monsieur Gilles Anache.

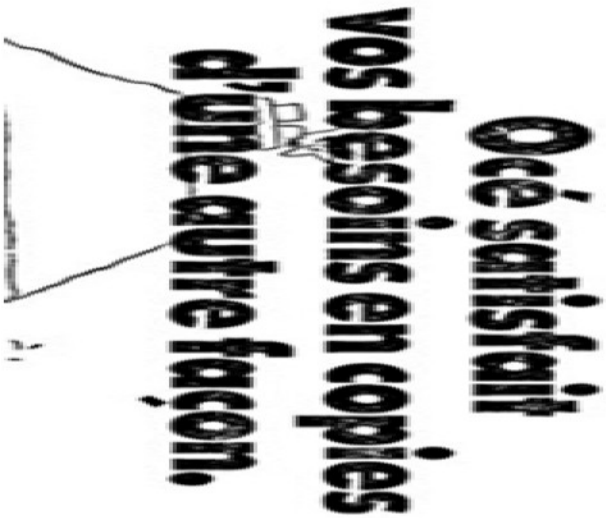
Afin de conclure, il est possible de s'interroger sur les évolutions juridiques futures nécessaires. L'essor de mouvements transhumanistes viendra-t-il remettre en cause les avancées actuelles ? L'homme 2.0 pourra-t-il conserver sa vie privée ?

137 "Internet, les nouveaux territoires de la liberté et de la vie privée", G. ACHACHE, Tout dire ? Transparence ou secret, Presses Universitaires de France « Hors collection », 2012, p 7-15.

ANNEXES

Annexe n°1 : Article dans le Monde sur le projet SAFARI

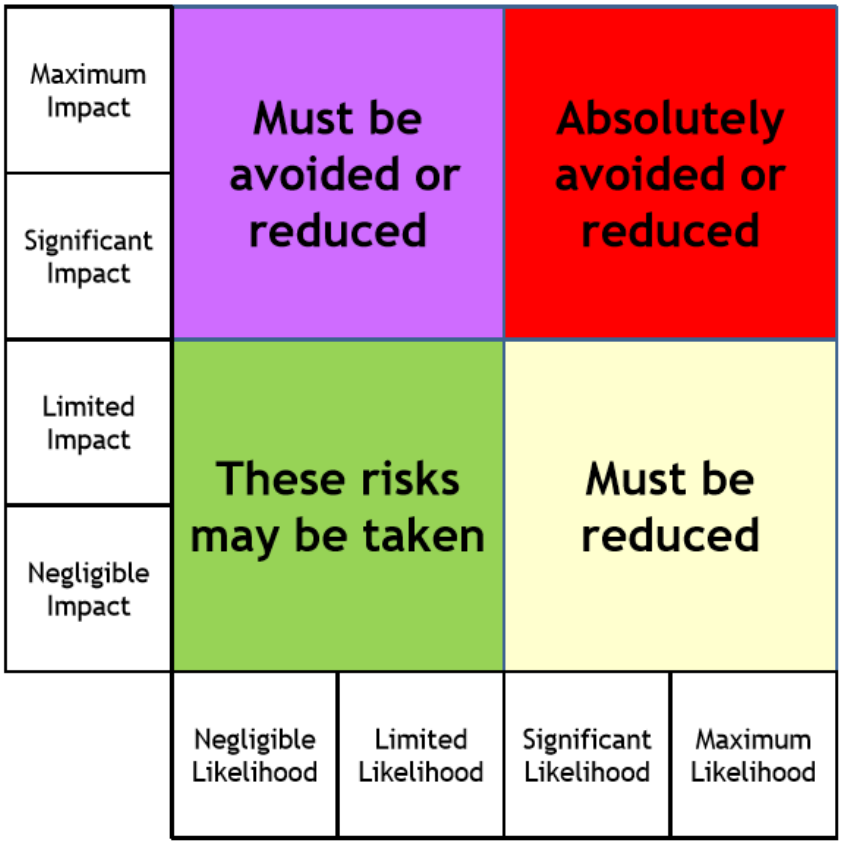




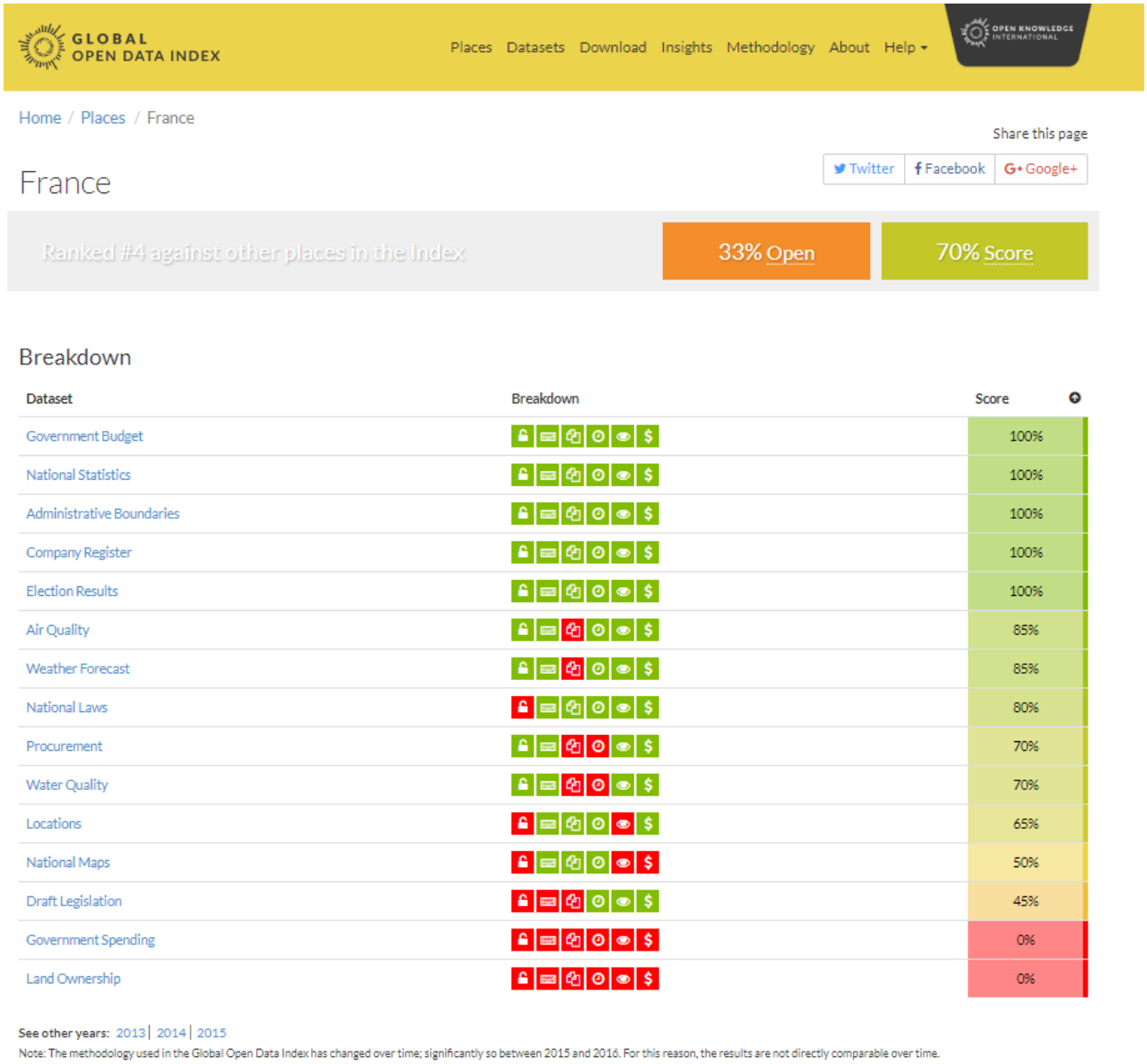
Annexe n° 2 : Exemple de « Risk Map » inspiré de la CNIL de Antonio KUNG

Risk map = F (likelihood, impact)

inspired from CNIL: https://www.cnil.fr/sites/default/files/typo/document/CNIL-ManagingPrivacyRisks-Methodology.pdf



Annexe n°3 : L'évaluation du niveau d'ouverture des données publiques en France par catégories selon GLOBAL OPEN DATA INDEX.



GLOBAL OPEN DATA INDEX

Places Datasets Download Insights Methodology About Help

Home / Places / France

Share this page

Twitter Facebook Google+

France

Ranked #4 against other places in the Index

33% Open

70% Score

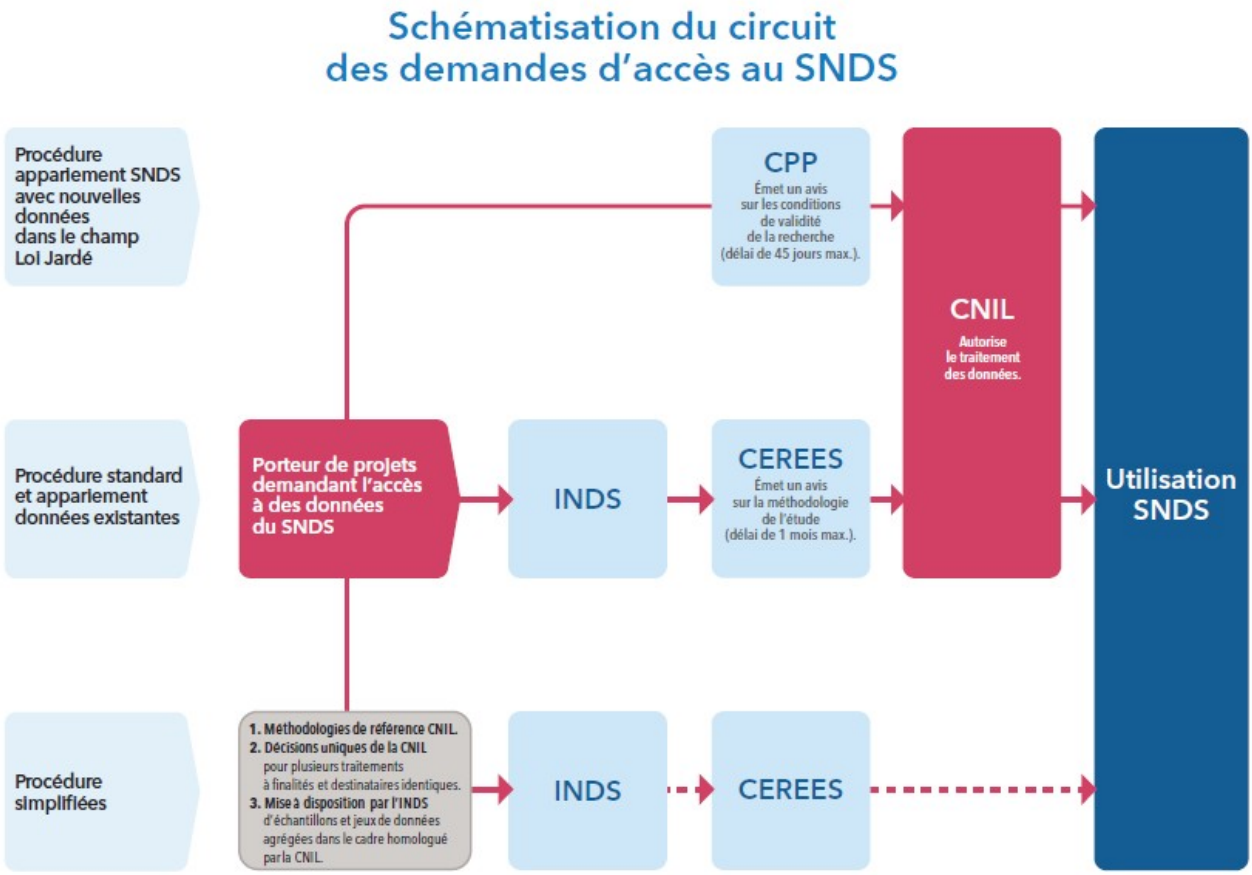
Breakdown

Dataset	Breakdown	Score
Government Budget		100%
National Statistics		100%
Administrative Boundaries		100%
Company Register		100%
Election Results		100%
Air Quality		85%
Weather Forecast		85%
National Laws		80%
Procurement		70%
Water Quality		70%
Locations		65%
National Maps		50%
Draft Legislation		45%
Government Spending		0%
Land Ownership		0%

See other years: 2013 | 2014 | 2015

Note: The methodology used in the Global Open Data Index has changed over time; significantly so between 2015 and 2016. For this reason, the results are not directly comparable over time.

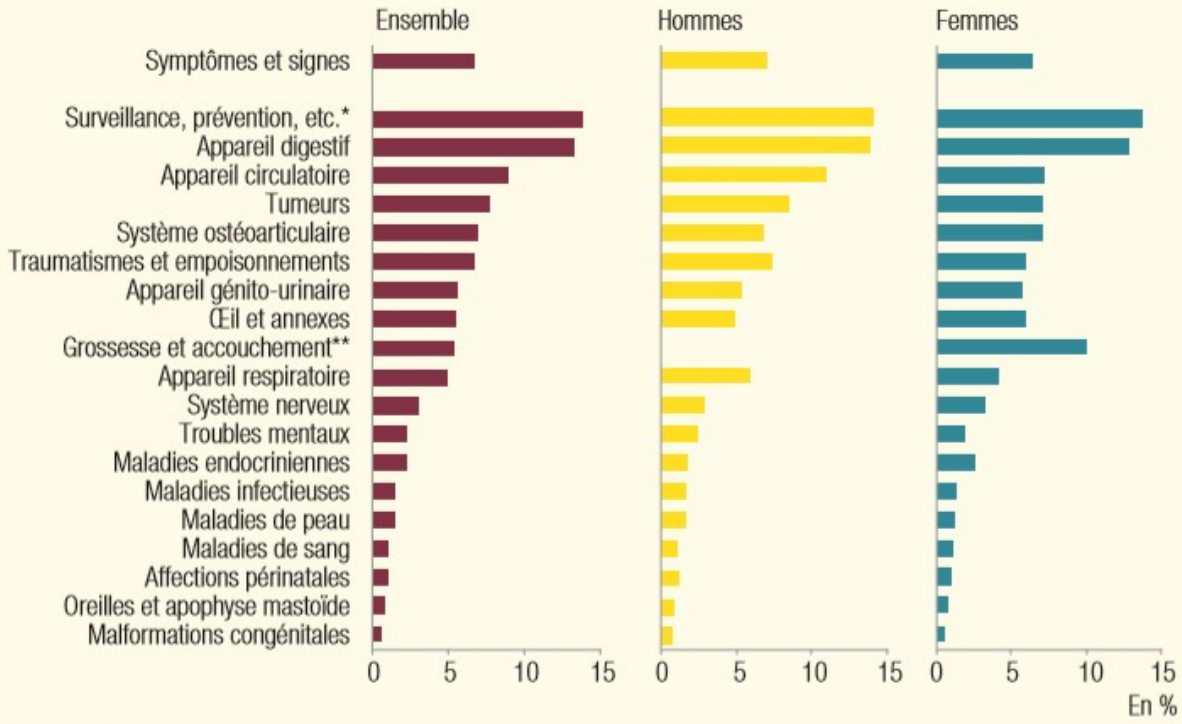
Annexe n°4 : Schématisation du circuit des demandes d'accès au SNDS. Source : site de la CNIL.



Annexe n°5 : Exemple d'un graphique suite à l'analyse des données sur le SNDS. Etude & Résultats, Dress « Hospitalisation de court séjour : quels motifs de recours en 2013 ».

GRAPHIQUE 3

Répartition des séjours annuels en 2013 selon le sexe du patient et la pathologie



* Motifs de recours aux services de santé autres que la maladie ou les traumatismes tels que surveillance, prévention, traitements itératifs, motifs sociaux (codes Z de la classification internationale des maladies [CIM] de l'Organisation mondiale de la santé [OMS] 10e révision).

** Non compris accouchement unique et spontané (code O80 de la CIM de l'OMS 10e révision).

Note • Diagnostic principal manifestation clinique, regroupement selon les chapitres de la CIM de l'OMS 10e révision. Ensemble des séjours appartenant à des hospitalisations en médecine, chirurgie, obstétrique et odontologie (MCO)≥ 24 heures (y compris pour des traitements itératifs) et des hospitalisations < 24 heures pour des motifs autres que dialyse, chimiothérapie, radiothérapie et autres traitements itératifs.

Champ • France hors Mayotte.

Sources • Base nationale PMSI-MCO scellée ATIH, exploitation DREES.

Bibliographie

Manuels et ouvrages généraux

- BEIGNIER B., BINET J-R, « *Droit des personnes et de la famille »*, Etudes, 2017.
- HENNETTE-VAUCHEZ Y. et ROMAN D., « *Droits de l'homme et libertés fondamentales »*, 3ème édition, Dalloz, 2017.
- LAUDE A., MATHIEU B., et TABUTEAU D., « *Droit de la santé »*. 3ème édition. Presses Universitaires de France, 2012.
- Le Lamy « *Droit numérique »,* 2017.
- MOQUET-ANGER M.L., « *Droit hospitalier »*, LGDJ, 5ème édition, 2018.
- TRUCHET D., « *Droit de la santé publique »,* 9ème édition, Dalloz, 2016.

Ouvrages spécialisés et thèses

- APOLLIS B. (dir.), « *L'hôpital public au début du XXIème siècle* », RDSS, 2015, numéro Hors Série.
- BINET J-R., « *Droit et progrès scientifique. Science du droit, valeurs et biomédecine* », Presses Universitaires de France, 2002.
- BLAIZOT-HAZARD C., « *NTIC, secret et droits fondamentaux* », 2017.
- MATHY C., « L*'innovation disruptive dans les systèmes de santé* », Thèse, 2011.
- TINOT-THOMAS G. « *Les sources du droit médical* », Thèse, 2004.

Dossiers :

- *« Données de masse en santé »,* Journal international de bioéthique et d'éthique des sciences 2017/3, Vol. 28.
- « *Ecosystème de santé : les nouveaux modes de régulation de l'information* », I2D – Information, données & documents, 2016/3, Vol. 53
- « *Open et big data* », Informations sociales 2015/5, n° 191.
- *« Télémédecine »,* Journal International de Bioéthique 2014/3, Vol. 25.

Rapports et avis

- 1998, G. BRAIBANT, « *Rapport sur les données personnelles et société de l'information* »
- 2000, Institute of Medicine (US) Committee on the Role of Institutional Review Boards in Health Services Research Data Privacy Protection, « *Protecting Data Privacy in Health Services Research* ». Washington (DC): National Academies Press (US);
- 2002, révisé en 2016, « *Déclaration de l'Association médicale mondiale sur les considérations éthiques concernant les bases de données de santé et les biobanques* ».
- 2008, Avis du CCNE n°104, « *Le dossier médical personnel et l'informatisation des données de santé* ».
- 2009, Haut conseil de la Santé publique, « *Les systèmes d'information pour la santé publique* ».
- 2012, Haut conseil de la Santé publique, « *Pour une meilleure utilisation des bases de données nationales pour la santé publique et la recherche* », Collection Documents
- 2014, Rapport du Conseil d'État, « *Le numérique et les droits fondamentaux* ».
- 2014, Rapport Commission open data en santé.
- 2014, Commission européenne « *Open Data in Health: how knowledge may generate trust* ».
- 2015, Conseil National de l'Ordre des médecins, « *Livre blanc : De la e-santé à la santé connectée* ».
- 2016, IRDES « *E-santé : télésanté, santé numérique ou santé connectée* ».
- 2016, Ministère chargé de la santé, « *Stratégie nationale pour le développement de l'e-santé* ».
- 2016, GREENBERG C. J., NARANG S., « *World Health Organization Member States and Open Health Data: An Observational Study* », Epidemiology Biostatistics and Public Health - Volume 13, Number 3
- 2017, Septièmes entretiens du Conseil d'État en droit social, « *Santé et protection des données* ».

› 2017, Délibération de la CNIL n° 2017-022 du 26 janvier 2017 portant avis sur un projet d'arrêté relatif au référentiel de sécurité applicable au Système national des données de santé.

Articles

- BERANGER J., « *E-santé, m-health, big data médicaux : Vers une hiérarchisation des données médicales. »* Revue Hospitalière De France, 562, p. 70-74, 2015.
- BICLET P., « *Éditorial Secret et e-santé* », Médecine & Droit, 2013 p.3-4.
- BOSSI J., « *Comment organiser aujourd'hui en France la protection des données de santé* » RDSS 2010 p.208.
- BROSSET E., « *Le droit à l'épreuve de la e-santé : quelle « connexion » du droit de l'Union européenne ?* », RDSS, n°5, 2016, 869.
- CAPODANO J., « *Dossier médical partagé (DMP) et secret professionnel : les nouveaux enjeux ?* », Revue droit et santé, n°76, 2017.
- COLLOC J. et HENOCQUE B., « *Introduction - Enjeux du big data et identifications des données médicales* », Les Cahiers du numérique, vol. 12, n°1, p. 9-12, 2016.
- DEBIES E., « *L'ouverture et la réutilisation des données de santé : panorama et enjeux* », RDSS, 2016, p.697.
- DE MAISON ROUGE O., « *Décryptage sur la protection juridique des informations sensibles Du régime des données personnelles à la confidentialité des informations économiques non divulguées* » Dalloz IP/IT, 2017, p.273.
- DUROUSSEAUD J.-C., « *Numérique en santé. Télémédecine. Homo connectus.* » Revue Hospitalière De France, 561, p. 26-27, 2014.
- EON F., « *Hôpital public et données personnelles des patients* » RDSS 2015 p.85
- GAMBARDELLA S., « *Une lecture de la jurisprudence de la Cour européenne des droits de l'Homme relative aux données de santé* », RDSS, 2016, p.271.
- GAUMONT-PRAT H., « *Aspects éthiques de l'informatisation des données de santé dans la société de l'information* » Recueil Dalloz 2001 p.1432
- GHARBI L., et al. « *Ouverture de la journée "Enjeux et opportunités du numérique. »* Dossier, Regards De La Fhp, 34, p. 6-37, 2015.
- LACOUR S., « *Du secret médical aux dossiers de santé électroniques. Réflexions*

juridiques sur la protection des données de santé », Médecine & Droit, 2016, p. 62–69.

- MARTIAL-BRAZ N., « *Le renforcement des droits de la personne concernée* », Dalloz IP/IT, 2017, p.253.
- MORLET-HAIDARA L., « *Le système national des données de santé et le nouveau régime d'accès aux données* », RDSS, 2018, p.91.
- NIETO A., « *« Santé » et « Big data » : Google à l'origine d'une nouvelle ère d'encadrement des données personnelles de santé ?* », Revue droit & santé n°67, 2018
- PISANIA E., ABOUZAHRB C., « *Sharing health data: good intentions are not enough* », Bull World Health Organ, 2010, 88, p.462-466
- ZORN-MACREZ C., « *Chronique martienne » des données de santé numérisées. Brèves observations sur une réglementation surréaliste »*, Revue droit et santé n°36, 2010

Site web :

- https://www.cnil.fr/
- https://www.has-sante.fr/portail/
- https://www.data.gouv.fr/fr/
- https://www.snds.gouv.fr/SNDS/Accueil
- http://www.claytonchristensen.com/key-concepts/ de Clayton Christensen, vu le 23/06/2018.

Divers

- Colloque de l'AFDS, « Le droit des données de santé », 2004

Table des matières

Remerciements.....I
Dédicace.....II
Sommaire.....III
Liste des abréviations.....IV

INTRODUCTION.....1

PARTIE I – Une législation sur la protection des données de santé influencée par celle des droits de la personne.....7

CHAPITRE I – Les droits fondamentaux de la personne.....8

SECTION I – La volonté de la personne.....9
§1 – Le consentement.....9
A – La recherche du consentement pour toute action.....9
B – Le patient réel acteur de sa prise en charge.....11
§2 – Information et opposition.....12
A – Le droit d'information.....12
B – Le droit d'opposition.....13

SECTION II – La vie privée de la personne.....16
§1 – La confidentialité.....16
A – Le secret des informations.....16
B – Vers affaiblissement du secret médical ?.....17
§2 – Le principe de non-discrimination.....19
A – Le principe.....19
B – Droit à l'oubli.....21

CHAPITRE II – Une protection renforcée, des garanties similaires.....23

SECTION I – Des principes déterminants autour de la prise en charge et du traitement.....24
§1 – Les principes autour de la justification de l'acte.....24
A – Le principe d'interdiction générale d'atteinte à la personne et de traitement données sensibles.....24
B – Le principe de loyauté.....25
§2 – Les principes autour des conditions de l'acte.....26
A – Le principe de finalité.....27

B – Le principe de proportionnalité.....28

SECTION II – L'encadrement par des autorités spécialisées.....30
§1 – Les autorités de contrôle.....30
A – La création et leur rôle.....30
B – Leurs différences.....31
§2 – Les moyens.....32
A – L'utilisation de normes de soft law pour encadrer les pratiques.....32
B – Du passage de l'accréditation à la certification.....34

PARTIE II – Des différences croissantes remettant en cause la continuité ?.....36

CHAPITRE I – Des particularités propres aux données.....37

SECTION I – La question de la propriété des données.....38
§1 – La non patrimonialité.....38
A – Le principe de non patrimonialité.....38
B – Un principe plus discuté pour les données.....40
§2 – L'autodétermination informationnelle.....41
A – La notion d'autodétermination informationnelle.....41
B – La portée juridique.....43

SECTION II – La dématérialisation des données.....45
§1 – Du matériel à l'immatériel : changement de paradigme.....45
A – Une des principales limites du rapprochement des deux systèmes juridiques.....45
B – Le big data en santé.....47
§2 – Le cas spécifique des innovations disruptives.....48
A – La notion "d'innovation disruptive" en santé.....48
B – La remise en cause de principes juridiques traditionnels.....49

CHAPITRE II – Quelle protection des données pour l'avenir ?.....52

SECTION I – La pertinence d'un renforcement de la protection des données de santé semblable à la protection de la personne ?.....53
§1 – Les avantages d'un renforcement au nom de la continuité.....53
A – Un meilleur contrôle par l'individu de ses données.....53
B – Moins de risque d'une utilisation inappropriée par les tiers.....54
§2 – Les risques si renforcement au nom de la continuité.....55
A – Les conséquences et responsabilités du patient dans la « gestion de ses données ».....56
B – De surprotection de l'individu au détriment de la santé collective ?.....57

SECTION II – Vers une rupture de continuité ?.....59
§1 – La philosophie de l'ouverture des données.....59
A – Des textes européens et nationaux qui prône la circulation et l'ouverture des données.....59
B – Le SNDS : l'open data des données de santé.....61
§2 – Propositions de conciliations.....62
A – Un nécessaire consensus international.....62
B – Quelques pistes particulières.....63

CONCLUSION.....66

Annexes.....68
Bibliographie.....73
Table des matières.....74

Aujourd’hui, les données de santé se multiplient et se démultiplient. La société numérique a développé les moyens de les faire proliférer. Une protection juridique a donc rapidement été perçue comme une nécessité à l’aube des progrès technologiques afin de protéger des droits et libertés fondamentales. Le régime juridique des données de santé s’est alors inspiré de nombreux mécanismes traditionnels du droit des personnes ainsi que du droit médical.

Les différentes législations autour des données doivent s’adapter aux évolutions technologiques toujours plus innovantes. Le régime juridique des données de santé n’y échappe pas. Il se dissocie alors progressivement des canons juridiques traditionnels et les bouscule à divers égards.

Mots-clés : Autodétermination informationnelle – Big data – CNIL – Donnée de santé – Données personnelles – Droit des données – Droits de la personne – Droits fondamentaux – E-santé – HAS – Libertés fondamentales – Nouvelles technologies – Open data – Système d’information de santé