LA PROTECTION ET LA VALORISATION DES DONNEES DE SANTE ET LE SERVICE PUBLIC HOSPITALIER

Rémi BOURY

Mémoire de recherche

Master 2 Droit et Politiques de Santé

Sous la direction de Madame le Professeur Johanne SAISON

Année universitaire 2018-2019

Remerciements

Ce mémoire a été écrit en grande partie grâce aux connaissances que j'ai pu acquérir lors de mon stage au sein du CHU de Lille. Aussi, j'aimerais avant tout remercier les personnes qui, durant ce stage, ont accepté de partager, avec patience et bienveillance, leurs connaissances de toutes natures.

Notamment, j'aimerais remercier l'équipe de l'entrepôt de données de santé du CHU de Lille (Projet Include) : le Dr. V. SOBANSKI, le Dr. G. FICHEUR, le Dr. D. THEIS, P. ANDREY, ainsi que M. CAILLIER, M.-A. ALLAIN, B. DERVAUX, de la Direction de la Recherche et de l'Innovation, F. LENOIR de la Direction des Affaires Juridiques, L. DELATTRE des Affaires Générales et Y.-F. DESCACQ du Département d'Information Médicale.

Je tiens également à remercier le Pr. Johanne SAISON, pour son soutien, ses conseils, ses connaissances, partagées avec passion durant ces deux années de Master, et pour avoir accepté de diriger ce mémoire.

Enfin, je tiens à remercier l'ensemble de mes proches, famille, amis et amour, qui ont eu à supporter mon mauvais caractère et mon manque de disponibilité pendant la rédaction de ce mémoire.

Mes regards se tournent maintenant vers Rennes, où je pars préparer le concours de directeur d'hôpital, en espérant voir mes efforts récompensés !

Principales abréviations

AAI Autorité Administrative Indépendante

AJDA Actualité juridique de droit administratif

al. alinéa

ANSP Agence Nationale de Santé Publique (Sante Publique France)

API Autorité Publique Indépendante

Art. Article

ASIP Santé Agence des Systèmes d'Information Partagés de Santé

Bull. Ordre méd. Bulletin de l'Ordre des médecins

CA Cour d'appel

CAA Cour administrative d'appel

Cah. hosp. Les Cahiers hospitaliers

CASF Code de l'action sociale et des familles

Cass. Ass. plén. Cour de cassation, Assemblée plénière

Cass. ch. mixtes Cour de cassation, chambres mixtes

Cass. civ. Cour de cassation, chambre civile

Cass. com. Cour de cassation, chambre commerciale

Cass. crim. Cour de cassation, chambre criminelle

Cass. req. Cour de cassation, chambre des requêtes

Cass. soc. Cour de cassation, chambre sociale

C. civ. Code civil

CE Conseil d'Etat

CEDH Cour européenne des droits de l'homme

CGCT Code général des collectivités territoriales

ch. chambre

chron. chronique

CJCE Cour de justice des communautés européennes

CNAM Caisse Nationale d'Assurance Maladie

CNIL Commission Nationale de l'Informatique et des Libertés

CNOM Conseil National de l'Ordre des Médecins

coll. collection

comm. commentaire

concl. conclusion

CP Code pénal

CSP Code de la santé publique

CSS Code de la sécurité sociale

CT. Code du travail

DMP Dossier Médical Partagé ou Personnel

éd. édition

fasc. fascicule

Gaz. Pal. Gazette du Palais

GHT Groupement Hospitalier de Territoire

HADOPI Haute Autorité pour la Diffusion des Œuvres et la Protection des droits sur Internet

HAS Haute Autorité de Santé

Ibid. Ibidem au même endroit

INDS Institut National des Données de Santé

infra voir ci-dessous

INVS Institut National de Veille Sanitaire

J. Cl. Juris-Classeur

JCP G La semaine juridique, édition générale

JO Journal officiel

JOUE Journal officiel de l'union européenne

JP jurisprudence

LGDJ Librairie générale de droit et de jurisprudence

loc. cit. à l'endroit cité

Méd. et droit Médecine et Droit

n° numéro

NIR Numéro d'Inscription au Répertoire

op. cit. dans l'ouvrage précité

Ord. Ordonnance

p. page

LPA Les Petites Affiches

préc. précité

PUF Presses universitaires de France

RDSS Revue de droit sanitaire et social

Rép. Civ. Dalloz Répertoire civil Dalloz

RFAP Revue française d'administration publique

RFAS Revue française des affaires sociales

RFDA Revue française de droit administratif

RGDM Revue générale de droit médical

SNIIRAM Système National d'Information Inter-Régimes de l'Assurance Maladie

SNDS Système National des Données de Santé

supra voir ci-dessus

T.A Tribunal administratif

TC Tribunal des conflits

TGI Tribunal de grande instance

TI Tribunal d'instance

Introduction

« Nous vivons une période de rupture dont on ne perçoit encore que le début. Pratiques médicales, relation entre médecin et patient, recherche, organisation des soins… Tout va être profondément modifié. »[1]

Jean-François DELFRAISSY, président du Comité consultatif national d'éthique, sur les évolutions numériques et l'utilisation des « données massives » en santé.

La révolution numérique et l'explosion quantitative et qualitative des données personnelles ont fait naître, au sein de la société, de nouvelles possibilités, et en conséquence de nouveaux marchés économiques. Ces données, dont la valeur est estimée à 1000 milliards de dollars pour les seules données européennes, d'ici 2020[2], connaissent de nombreuses applications.

Le secteur de la santé et en premier lieu les hôpitaux sont notamment intéressés par l'intelligence artificielle (IA) et les innovations technologiques qu'elle porte : amélioration de la prévention, amélioration de la fiabilité des diagnostics, précision des traitements, facilitation de l'observance, mais également amélioration de la gestion des flux, diminution des dépenses par l'amélioration de l'efficience des soins et l'automatisation de certaines tâches ou encore amélioration de la relation patient-soignant.

Avec un marché actuel de 4 milliards de dollars et 60 milliards de dollars attendus d'ici 2025[3], l'IA est un sujet majeur et éminemment stratégique de nos jours. En conséquence, cette

---

[1] BELOT Laure, « Jean-François Delfraissy : "Les usagers ont un droit sur leurs données de santé" », Le Monde, 04 Juin 2019.

Accessible en ligne : https://www.lemonde.fr/sciences/article/2019/06/04/jean-francois-delfraissy-les-usagers-ont-un-droit-sur-leurs-donnees-de-sante_5471356_1650684.html

[2] ANOHORY Michèle, CHU Robert, NORMAND Alexis, SPREUX Oliver, « Il faut inventer un droit patrimonial sur ses données de santé », tribune dans « Le Monde », 11 Janvier 2019.

[3] OMARJEE Sulliman, « Le principe de disponibilité des données publiques : mythe ou réalité ? », 15 Novembre 2003, sur le site http://www.droit-ntic.com/

innovation technologique est saisie à la fois par entreprises privées et par les politiques publiques, qui la prennent en compte dans leurs projets de développement.

Ainsi, le 28 mars 2018, le député de l'Essonne et mathématicien lauréat 2010 de la médaille Fields, Cédric VILLANI, présentait son rapport « *Donner du sens à l'intelligence artificielle : pour une stratégie nationale et européenne* »[4], dans lequel il menait une large réflexion sur l'intelligence artificielle (IA) et affirmait que la France disposait d'un fort potentiel en la matière, malgré une certaine difficulté à transformer ses avancées scientifiques en applications industrielles et économiques. La question de la valorisation de la recherche et du transfert de technologie était ainsi posée, avec d'autant plus d'intensité qu'elle mène parfois à la fuite des cerveaux français vers l'étranger.

Les questions d'éthique étaient également abordées au sein du rapport, indissociables du sujet de l'intelligence artificielle et de l'usage de données, du fait du potentiel extraordinaire de l'intelligence artificielle qui permet de développer des applications reposant sur une capacité d'analyse infiniment supérieure à celle des humains.

D'autre part, le rapport identifiait quatre secteurs prioritaires dans lesquels la France devait particulièrement concentrer son effort de développement de l'intelligence artificielle : la santé, les transports, l'environnement et la défense.

Le jour suivant, le 29 mars 2018, le Président de la République, Emmanuel MACRON, présentait au Collège de France sa vision et sa stratégie pour faire de la France un pays leader de l'intelligence artificielle. A la suite de la remise du rapport Villani, le Président de la République annonçait ainsi, dans sa continuité et selon la proposition faite par Cédric VILLANI, la création d'une plateforme appelée « *Health Data Hub* » comme un des points forts de la stratégie IA

Accès direct : http://www.droit-tic.com/pdf/dispo_dp.pdf

[4] VILLANI Cédric, Rapport « Donner du sens à l'Intelligence Artificielle : pour une stratégie nationale et européenne », 28 mars 2018, La documentation Française.

française. La Ministre des Solidarités et de la Santé Agnès BUZYN lançait, en conséquence, une mission de préfiguration de cette plateforme d'exploitation des données de santé le 12 juin 2018. Cette mission, pilotée par trois experts (Dominique POLTON, présidente de l'Institut national des données en santé (INDS), Marc CUGGIA, professeur d'informatique médicale et praticien hospitalier au CHU de Rennes et Gilles WAINRIB, président fondateur de la start-up Owkin) et incluant également des représentants de la recherche, de l'écosystème des start-ups, de l'industrie, des professionnels et établissements de santé, de l'administration et de l'Assurance Maladie, remettait ainsi son rapport le 12 octobre 2018[5]. Celui-ci contenait notamment une feuille de route pour la mise en œuvre opérationnelle de la plateforme, ainsi que des recommandations, notamment sur les aspects organisationnels et réglementaires pour qu'elle puisse se dérouler dans un contexte favorable.

La Ministre confirmait, au premier trimestre 2019, la mise en place du « Health Data Hub » d'ici la fin de l'année, et confiait au directeur de la DREES, Jean-Marc AUBERT, cette mission.

Afin que ce projet de grande ampleur soit mené à bien, des réformes juridiques et organisationnelles étaient indispensables. C'est pourquoi des travaux législatifs ont été entrepris et sont actuellement en cours[6], afin d'adapter le droit à la volonté politique de développer le domaine de l'intelligence artificielle et l'exploitation des données de santé[7] en général, dans le cadre du plan « Ma Santé 2022 »[8].

---

[5] CUGGIA Marc, POLTON Dominique, WAINRIB Gilles, COMBES Stéphanie, Rapport « Health Data Hub – Mission de préfiguration », Ministère de la Santé et des Solidarités, Octobre 2018.

[6] Au premier semestre 2019.

[7] A travers le projet de loi relatif à l'organisation et à la transformation du système de santé.

[8] « Dans son discours du 18 septembre 2018 adressé au monde de la santé, le président de la République a donné des orientations claires et fortes pour répondre concrètement aux difficultés des patients et à celles que rencontrent les professionnels, mais aussi pour inventer le système de santé des 20 prochaines années. […]

Ces différents rapports et ces différentes décisions politiques traduites au sein de différents projets de lois illustrent la volonté du gouvernement français d'agir de manière ambitieuse et réelle dans le domaine des données, du « Big Data », de l' « Open Data », de l'intelligence artificielle, notamment dans le domaine de la santé, comme en témoigne la création déjà relativement avancée du Health Data Hub et des entrepôts de données de santé locaux (AP-HP, CHU de Rennes, Bordeaux, Lille…). La santé constitue ainsi une des priorités sur lesquelles la France souhaite concentrer son effort de développement en matière d'IA.

Au centre de ces volontés politiques et de ces projets de réformes se trouvent les algorithmes, mais surtout les données, les « data », matière première indispensable à la mise au point d'outils d'IA. Dans le domaine de la santé, ce sont les données de santé qui prennent ainsi de plus en plus d'importance – économique, stratégique, éthique, juridique… – et des réflexions majeures ont lieu, actuellement, à leur sujet.

Il s'agira donc, dans un premier temps introductif, de définir les contours de notre sujet d'étude – données de santé, big data, open data, IA dans le domaine de la santé – (I) pour ensuite présenter le cadre dans lequel s'inscrivent les réflexions dans ce domaine afin d'en exprimer les enjeux, les défis et les problématiques à la fois juridiques, économiques et éthiques, notamment dans le cadre spécifique du service public hospitalier (II).

Pour porter certaines de ces mesures, le projet de loi Ma Santé 2022 est présenté en commission des affaires sociales de l'Assemblée nationale le 5 mars, puis en session plénière à partir du 18 mars. »

Source : https://solidarites-sante.gouv.fr/systeme-de-sante-et-medico-social/ma-sante-2022-un-engagement-collectif/article/ma-sante-2022-mise-en-oeuvre

I. Les données de santé, de la subtilité d'un objet complexe

La notion de « données de santé », pour les professionnels impliqués dans ce domaine, peut sembler relativement simple, basique. En réalité, définir cet objet d'étude s'avère être une tâche ardue, au regard d'une part de la pluralité des aspects de la notion, à la fois dans sa conception et dans ses applications.

A. Les données de santé et la complexité de définir une notion polymorphe.

Dans l'univers de la santé, les données numériques se multiplient. Ces données de santé, devenant de plus en plus précieuses et utiles, font l'objet de vifs débats autour de leur définition, laquelle devient un enjeu stratégique.

La «donnée» au sens étroit du terme, selon la définition de la circulaire du 14 février 1994 relative à la diffusion des données publiques, est « une information formatée pour être traitée par un système informatique. Elle sera entendue au sens large d'information collectée ou produite sur n'importe quel support ». Néanmoins, avec le temps, la notion de « donnée » s'est élargie dans la pratique, et cette première tentative de définition ne suffisait plus. Au surplus, dans le contexte européen, la multiplié des conceptions relatives à la notion de donnée devenait problématique.

C'est ainsi que le 27 avril 2016, à travers le Règlement Général relatif à la Protection des Données (RGPD)[9], les autorités européennes, après de longs débats[10], ont fixé un cadre commun aux différents pays de l'Union Européenne (UE) en matière de protection des données personnelles.

[9] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).

[10] Le texte a été voté après quatre années de négociation entre la Commission et le Parlement européens.

Applicable depuis mai 2018, le RGPD définit ainsi de manière large les données concernant la santé (type particulier de « donnée personnelle ») comme toute information se rapportant à une personne physique identifiée ou identifiable (directement ou indirectement) « relative 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 »[11].

Il est intéressant de noter que le RGPD distingue, dans leurs définitions, les données concernant la santé, les données génétiques (relatives aux caractéristiques génétiques héréditaires ou acquises d'une personne physique qui donnent des informations uniques sur la physiologie ou l'état de santé) et les données biométriques (résultant d'un traitement technique spécifique, relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique)[12], sans pour autant opposer ces notions.

Ainsi, on peut considérer qu'une donnée de santé est une donnée se rapportant à l'état de santé, physique ou mental, passé, présent ou futur, d'une personne physique identifiée ou identifiable. Cette donnée peut être collectée à l'occasion d'une prestation de soins de santé, d'une prise en charge sanitaire ou pour la recherche. Certaines données ne sont pas des données de santé par nature (activité physique, alimentation…), mais elles deviendront des données de santé par destination dès lors qu'elles peuvent permettre de déduire un état de santé après avoir été croisées à d'autres données (âge, sexe, alimentation…).

On observe en conséquence une grande disparité des données de santé, corrélée à leur quantité qui croit de manière exponentielle ces dernières années (le volume mondial de données de santé est estimé à 2,3 milliards de giga-octets d'ici 2020[13]). En effet, les données de santé peuvent revêtir

---

[11] Article 4, notamment le point 4.15 du RGPD.

[12] Respectivement aux articles 4.15, 4.13 et 4.14 du RGPD.

[13] SOL Hélène, « Big Data en santé : données concernées, usages, entrepôt bio-hétérogènes et outils d'exploitation (Avis d'experts) », ANAP, 07 Janvier 2016.

de nombreux aspects, que ce soit au niveau de leur typologie – donnée environnementale, démographique, comportementale, sociale, biologique, clinique… –, de leur source – essais cliniques, base de données médico-administratives, cohortes, registres, dossier médical, données patients obtenues grâce à des objets connectés, données d'opinion obtenues grâce à des moteurs de recherche ou des sites internet… – de leur format – données textuelles, valeur numérique, signal, imagerie, séquence génomique… – ou encore de leur caractéristiques – donnée individuelle ou agrégée, recueil prospectif ou rétrospectif, cohorte ouverte ou fermée, donnée structurée ou non-structurée, donnée accessible ou non-accessible… Il est donc impossible d'énumérer de manière exhaustive les différentes données relatives à la santé. Toutefois, nous comprendrons ici comme « données de santé » toute donnée ayant trait à la santé et au bien-être physique, mental et social (en nous fondant sur la définition typique de l'Organisation Mondiale de la Santé[14]), d'une personne physique identifiée ou identifiable.

De plus, ayant dit cela, il est possible d'identifier quatre natures différentes de données de santé : les données personnelles, par opposition aux données anonymes, les données anonymisées (des données personnelles rendues anonymes), et enfin les données publiques qui transcendent les classifications précédentes. Cette distinction sera étudiée plus en détail plus après.

D'autre part, les données de santé n'ont, individuellement, qu'une faible valeur ; c'est leur nombre, leur volume qui fait leur intérêt. On parle alors de « *Big Data* », de mégadonnées ou de données massives en santé, réunies au sein de banques de données. Selon la définition consacrée de Gartner[15], l'ensemble de données doit obéir à la règle des 3V pour être qualifié de « Big Data » : Volume, Variété, Vélocité. L'ensemble doit contenir un nombre très important de données, non

[14] La constitution de l'OMS, adoptée par la Conférence internationale de la Santé à New York le 22 juillet 1946, définit la santé comme « un état de complet bien-être physique, mental et social, et ne [consistant] pas seulement en une absence de maladie ou d'infirmité ».

[15] Gartner est une entreprise majeure dans le domaine des technologies de l'information, et tient un glossaire accessible en ligne : https://www.gartner.com/it-glossary/big-data/ (consulté le 15/05/2019).

traitable par un outil classique (volume), les données doivent être variées et provenir de sources différentes, pas toujours structurées (variété), et enfin les données doivent être créés, collectées et partagées à une vitesse forte (vélocité).

B. Les données de santé, objet aux applications multiples et éminemment stratégiques

Les données de santé, une fois convenablement qualifiées, ordonnées, peuvent faire l'objet de nombreuses utilisations et réutilisations. Les données de santé, en cela, apparaissent comme une matière première indispensable au développement d'outils d'amélioration du système de santé, de la médecine actuelle. L'exploitation et l'analyse de ce patrimoine immatériel constitué de jeux de données volumineux, couplée à l'utilisation des différentes formes d'IA permettent, par exemple, de développer et d'améliorer les outils de prévention, de diagnostic ou de soins, en tant que composante essentielle des sciences et technologies du numérique, en particulier de l'apprentissage machine, de la robotisation et des nouveaux moyens de communication.

Les champs d'application du big data en santé sont en effet multiples, et concernent ainsi la recherche en santé – pour qui le big data est une source presque inépuisable de nouvelles connaissances, indispensables à l'innovation et aux progrès médicaux les soins –, les activités de prévention et de diagnostic, mais également le pilotage du système de santé ou la gestion des établissements.

Pierre DELMAS-GOYON explique que « ces données peuvent être utilisées à des fins de recherche, pour prodiguer des soins, mais aussi à des fins commerciales par des nouveaux acteurs du numérique sur un marché d'exploitation du bien-être »[16].

Plus précisément, le big data en santé permet, grâce aux avancées de la recherche médicale conjuguées aux progrès réalisés dans le domaine de l'intelligence artificielle, le développement d'un nouveau modèle médical, la médecine « 4 P », pour « Prédictive, Préventive, Personnalisée et Participative ». Dans ce cadre se développe alors la médecine prédictive (anticiper l'apparition ou l'évolution des maladies), la médecine de précision (améliorer et personnaliser les traitements administrés), la chirurgie assistée (augmenter le chirurgien pour accroître la précision de ses gestes), l'aide au diagnostic, la prévention, la pharmacovigilance, etc…

Les données massives en santé sont souvent (mais pas exclusivement) liées aux outils d'intelligence artificielle. Celles-ci sont collectées soit en interne, soit grâce à des données libres d'exploitation, appelées « *Open Data* ».

Le secteur de l'intelligence artificielle en santé est un domaine de recherche particulièrement prometteur et est actuellement en pleine expansion. S'il constitue un domaine privilégié de la recherche et du développement technologique en santé, de l'utilisation des données massives en santé, il n'en constitue pas pour autant une application exclusive.

Selon Marvin MINSKY, le terme correspond à « la construction de programmes informatiques qui s'adonnent à des tâches qui sont, pour l'instant, accomplies de façon plus satisfaisante par des

[16] BELOT Laure, « Jean-François Delfraissy : "Les usagers ont un droit sur leurs données de santé" », Le Monde, 04 Juin 2019.

êtres humains car elles demandent des processus mentaux de haut niveau tels que : l'apprentissage perceptuel, l'organisation de la mémoire et le raisonnement critique »[17].

Le développement de l'IA a débuté en 1950[18], avec le premier calculateur d'Alan TURING, dans l'optique de faire réaliser par des machines des tâches habituellement réalisées par des humains grâce à leurs capacités cérébrales, cognitives. Au fur et à mesure de l'amélioration de cette technique, avec la création de la première machine apprenante en 1957 par Franck ROSENBLATT, de la reconnaissance vocale en 1972 par Raj REDDY, de la reconnaissance d'écrits manuels en 1989 par Yann LECUN – qui portera quelques années plus tard, à partir de 2012, le développement du *deep learning* – deux courants se sont constitués. On distinguera ainsi, classiquement, l'IA forte et l'IA faible.

La première (IA forte), qui apparait particulièrement complexe voire impossible pour certains chercheurs de notre époque[19], vise à concevoir une machine capable de raisonner comme l'humain, capable non seulement de produire un comportement intelligent, mais d'éprouver une impression d'une réelle conscience de soi, de « vrais sentiments » et « une compréhension de ses propres

---

[17] Cette phrase aurait été prononcée par Marvin MINSKY à l'occasion d'un programme de recherche ayant abouti à l'organisation d'une série de réunions organisées à Dartmouth College (Etats-Unis) au cours de l'été de 1956. La demande d'obtention d'un soutien financier au programme, écrite l'été précédent, s'intitulait « A proposal for the Dartmouth summer research project on artificial intelligence ». Le nom du nouveau domaine de recherche y faisait sans doute sa première apparition. Cette demande était signée par John McCarthy (1927-2011), à qui on attribue la proposition du terme « Artificial Intelligence », Marvin Minsky (1927-2016), Nathaniel Rochester (1919-2001) et Claude Shannon (1916-2001).

[18] Source : Encyclopédie Larousse en ligne. Site internet :

https://www.larousse.fr/encyclopedie/divers/intelligence_artificielle/187257 (consulté le 09/05/19).

[19] Certains chercheurs affirment que la conscience requiert un support biologique et donc matériel (la conscience serait le propre des organismes vivants), d'autres comme Roger PENROSE pensent que l'IA forte est impossible avec des machines manipulant des symboles comme les ordinateurs actuels, mais possible avec des systèmes dont l'organisation matérielle serait fondée sur des processus quantique…

Les tenants de l'IA forte ne voient, globalement, pas d'obstacle de principe à créer un jour une intelligence consciente sur un support matériel autre que biologique : l'absence actuelle d'ordinateurs ou de robots aussi intelligents que l'être humain serait moins due à un problème d'outil que de conception.

raisonnements »[20], avec le risque supposé de générer une machine supérieure à l'homme et dotée d'une conscience propre, ce risque engendrant des craintes de la part de certains acteurs[21].

La seconde, l'IA faible, tient en une « reproduction de l'intelligence » : la machine simule l'intelligence, mais n'est pas intelligente en soi. Ces systèmes ont en commun d'être limités dans leurs capacités de création et d'adaptation : ils sont limités par nature et nécessitent une action humaine, manuelle, pour être développés et adaptés, notamment pour accomplir d'autres tâches que celles pour lesquelles ils ont été initialement conçus. Tous les systèmes d'IA actuellement existants sont considérés comme des intelligences artificielles faibles.

Cette IA faible repose sur l'utilisation de toutes les technologies disponibles pour concevoir des machines capables d'aider les humains dans leurs tâches et mobilise de nombreuses disciplines, de l'informatique aux sciences cognitives en passant par les mathématiques, sans oublier les connaissances spécialisées des domaines auxquels on souhaite l'appliquer (dans notre cas, les connaissances médicales).

Deux modèles d'IA peuvent ensuite être identifiés, reposant sur deux modalités de raisonnement différents : le premier sur la logique (système « symbolique »), le second sur la quantité d'information (approche « numérique »).

Le premier de ces modèles, l'approche « symbolique », repose sur des règles logiques (déduction, classification, hiérarchisation…) et a permis de développer des outils appelés « systèmes experts » car s'appuyant sur des connaissances d'experts, à savoir, dans le domaine médical, sur l'ensemble des connaissances médicales dans un domaine donné et une formalisation des raisonnements des

---

[20] André LE GARFF, Dictionnaire de l'informatique (1975).

[21] Comme Stephen HAWKING (« Hawking : "L'intelligence artificielle pourrait mettre fin à l'humanité" », Le Monde, 3 décembre 2014) ; Bill Gates (« Bill GATES est « préoccupé par la superintelligence » artificielle », Le Monde, 29 janvier 2015) ou encore Elon MUSK (« Les 37 projets d'Elon Musk contre les dangers de l'intelligence artificielle »), Le Monde, 6 juillet 2015).

spécialistes qui lient ces connaissances entre elles pour aboutir à un diagnostic. Les systèmes actuels, qualifiés d'aide à la décision, de gestion des connaissances ou d'e-santé, bénéficient de meilleurs modèles de raisonnement ainsi que de meilleures techniques de description des connaissances médicales, des patients et des actes médicaux que leurs ancêtres des années 1980 et ne cherchent plus à remplacer le médecin, mais à l'épauler dans un raisonnement fondé sur les connaissances médicales de sa spécialité.

Le second modèle, l'approche « numérique », repose quant à lui sur les données : le système cherche des régularités dans les données disponibles pour extraire des connaissances, sans modèle préétabli. Cette méthode, née avec le connexionnisme et les réseaux de neurones artificiels dans les années 1980, se développe aujourd'hui grâce à l'augmentation de puissance des ordinateurs et à l'accumulation des gigantesques quantités de données (le « big data »). La plupart des systèmes actuels procèdent par apprentissage automatique, une méthode fondée sur la représentation mathématique et informatique de neurones biologiques, selon des modalités plus ou moins complexes. Les algorithmes d'apprentissage profond (deep learning) par exemple, dont l'usage explose depuis une dizaine d'années, s'inspirent du fonctionnement cérébral : ils simulent un réseau de neurones organisés en différentes couches, échangeant les uns avec les autres. La force de cette approche est que l'algorithme apprend la tâche qui lui a été assignée par "essais et erreurs", avant de se débrouiller tout seul.

Des applications de deep learning existent en traitement d'images, par exemple pour repérer de possibles mélanomes sur les photos de peau, ou bien pour dépister des rétinopathies diabétiques sur des images de rétines. Leur mise au point nécessite de grands échantillons d'apprentissage : 50 000 images dans le cas des mélanomes, et 128 000 dans celui des rétinopathies, ont été nécessaires pour entraîner l'algorithme à identifier les signes de pathologies. Pour chacune de ces images on lui indique si elle présente ou non des signes pathologiques. A la fin de l'apprentissage, l'algorithme arrive à reconnaître avec une excellente performance de nouvelles images présentant une anomalie.

En effet, comme nous l'avons vu plus tôt, les données de santé peuvent être utilisées dans le cadre du développement d'applications basées sur le recours à l'IA, applications permettant notamment d'améliorer la qualité des soins : l'IA est en effet au cœur de la médecine du futur, avec les opérations assistées, le suivi des patients à distance, les prothèses intelligentes, les traitements personnalisés grâce au recoupement d'un nombre croissant de données, la médecine prédictive… Les chercheurs développent pour cela des approches et techniques multiples, du traitement des langues et de la construction d'ontologies, à la fouille de données et à l'apprentissage automatique.

Au surplus, il faut bien différencier l'intelligence artificielle, l'apprentissage automatique (*machine learning :* le fait de concevoir un système général capable d'apprendre seul à partir d'exemples à résoudre un problème donné) et apprentissage profond (*deep learning :* terme abrégé pour "apprentissage dans les réseaux de neurones profonds", il s'agit des méthodes d'apprentissage automatique utilisant les réseaux de neurones profonds) : l'intelligence artificielle englobe le *machine learning*, qui lui-même englobe le *deep learning*.

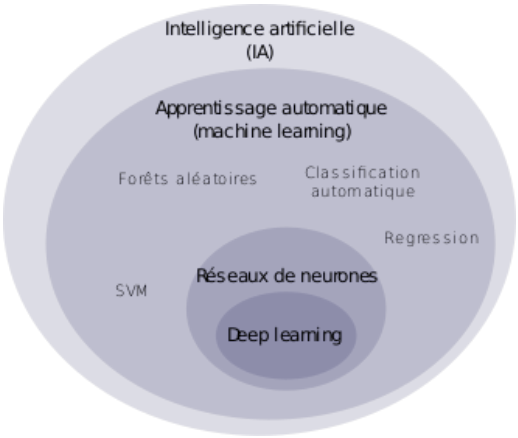

Schéma illustrant l'imbrication entre l'intelligence artificielle, le machine learning et le deep learning.

(Auteur : Bouliech – License creative common (CC BY-SA 4.0))

https://creativecommons.org/licenses/by-sa/4.0)

Les outils d'intelligence artificielle reposent donc sur l'accès à des données massives. En matière de données massives en santé, ces données peuvent provenir de nombreuses sources et revêtir de nombreux aspects. Ces différentes sources ainsi que les données qu'elles contiennent font l'objet, en France et ailleurs dans le monde, d'un encadrement spécifique, à la fois technique, institutionnel, juridique ou encore éthique, à la hauteur des enjeux qu'elles représentent.

II. L'encadrement des données de santé, le service public hospitalier, entre interventionnisme et laissez-faire

Bien que la volonté politique affichée soit celle d'une préoccupation croissante pour la question de la valorisation du patrimoine immatériel des personnes publiques, notamment de leurs données de santé, ce dernier domaine apparait comme étant toujours en cours de construction et fait l'objet de nombreuses interrogations de la part des professionnels du droit du fait de sa complexité.

Il induit en effet un recours à plusieurs sources juridiques, à la fois internationales (plus particulièrement communautaires : traités, règlements, directives de l'Union Européenne…) et nationales (comme, par exemple, la loi informatique et liberté de 1978 modifiée récemment en 2018, la loi de modernisation de notre système de santé de 2016 ou plus généralement les dispositions du code de la santé publique, de la propriété des personnes publiques, de la propriété intellectuelle, des relations entre le public et l'administration, les décrets, ordonnances, circulaires, textes parus ou en attente de parution, etc.).

A. Une apparente volonté d'action politique dans le domaine des données de santé

Historiquement, la France a commencé à s'intéresser aux données dès 1978, à travers la loi « Informatique et Libertés »[22] et la loi « CADA »[23].

La loi informatique et liberté entendait réguler, pour la première fois en France, au niveau européen, quelques temps après le land de Hesse (Allemagne) en 1971 et la Suède en 1973, les données et le traitement de données « nominatives » (*i.e.* à caractère personnel). La précocité de cette loi ainsi que le développement ultérieur d'Internet en ont fait un véritable « monument » juridique, pilier de la législation en matière numérique, ainsi qu'une inspiration pour les autres législations européennes (à la fois nationales et communautaires) élaborées plus tard.

Néanmoins, en 2004, la France sera le dernier pays membre à transposer une directive de 1995, transposition qui eut pour conséquence de modifier en profondeur la loi informatique et liberté, en remplaçant notamment le terme d'« informations nominatives », par « données à caractère personnel », et en les définissant (ce qui eut pour effet à la fois de réduire et d'élargir leur champ).

La loi « CADA », quant à elle, s'inscrit dans la droite lignée de l'article 15 de la Déclaration des droits de 1789, qui prévoit que « la société a le droit de demander compte à tout agent public de son administration », en octroyant un droit d'accès des citoyens aux documents administratifs et en mettant pour cela en place une « Commission pour l'Accès aux Documents Administratifs » (CADA). Ce droit d'accès, anachroniquement, constituait la première pierre d'un mouvement en faveur de l' « open data » concernant les données publiques.

---

[22] Loi n°78-17 du 6 Janvier 1978 relative à l'informatique, aux fichiers et aux libertés. Aussi dite « loi CNIL ».

[23] 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 fiscale. Aussi dite « loi CADA ».

Quelques années plus tard, cette loi fut complétée par la loi « DCRA »[24] qui avait pour objectif de d'améliorer la transparence, l'accessibilité et l'efficacité des administrations vis-à-vis des administrés. Cet objectif de transparence se traduisait en une harmonisation des dispositions issues des lois du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, du 17 juillet 1978 relative à l'accès aux documents administratifs et du 3 janvier 1979 sur les archives, tout en développant ces dispositions et les droits qui en découlaient pour les usagers. La loi affirmait ainsi, entre autres, le droit de toute personne à l'information, le droit de toute personne d'accéder aux informations « publiques » : communication des textes juridiques, des budgets et comptes des administrations, etc… L'administré, le public, l'usager, en tant que citoyen, devenait véritablement détenteur de droits vis-à-vis de l'administration, concernant notamment l'accès à l'information, lorsque celle-ci revêt un caractère public.

Le mouvement de l'administration vers l'open data, traduction de son devoir de transparence envers les administrés, était véritablement amorcé.

Selon la Commission Open Data[25], une stratégie d'open data appliquée au champ des données publiques de la santé « concernerait l'ensemble des données publiques qui ont vocation à être mises à la disposition de tous et réutilisées, au bénéfice de la santé publique, des patients et plus largement de l'information des usagers du service public de la santé. […] Prioritairement, il importerait d'ouvrir et de partager des données susceptibles de présenter un enjeu démocratique. A cet effet, les séries complètes, les données permettant de construire des référentiels, les données fréquemment actualisées, les données géolocalisées ou encore les données portant sur la transparence de l'action publique sont particulièrement utiles pour répondre à l'attente des citoyens. Ces informations ont vocation à être présentées sous un format permettant leur traitement

[24] Loi n°2000-321 du 12 Avril 2000 relative aux droits des citoyens dans leurs relations avec les administrations.

[25] Définition issue du débat thématique « Open Data en Santé – Réunion de la Commission Open Data du 19 Décembre 2013 ».

automatisé et leur réutilisation libre et gratuite, diffusées à une granularité la plus fine possible, dans le respect le cas échéant des lois en vigueur et notamment de la loi sur le secret statistique. Par ailleurs, elles ont vocation à s'appuyer sur des référentiels partagés et des nomenclatures décrites et publiées ».

En matière de santé, la génération de bases de données gérées par des entités publiques a connu un développement dès 1996, avec la généralisation du PMSI (programme de médicalisation des systèmes d'information)[26], à travers les ordonnances dites « Juppé »[27], dans le cadre de la réforme du système de santé. Le PMSI vise à définir l'activité des unités du service public hospitalier pour calculer leurs allocations budgétaires : depuis 2005, le PMSI est utilisé pour la mise en œuvre de la tarification à l'activité (T2A), système de rémunération des hôpitaux basé sur leur activité. Aujourd'hui, et depuis sa création en 2000, l'ATIH (Agence technique de l'information sur l'hospitalisation), établissement public de l'État à caractère administratif, centralise les données du PMSI, données concernant les séjours à l'hôpital. L'agence est ainsi chargée de la collecte, l'hébergement et l'analyse des données des établissements de santé (activité, coûts, organisation et qualité des soins, finances, ressources humaines…), mais aussi de gérer les classifications médico-économiques, les études de coûts, la restitution des informations, et participer à l'élaboration des nomenclatures de santé.

Le SNIIRAM (Système National Informatique Interrégimes d'Assurance Maladie) fut quant à lui créé par la loi du 23 décembre 1998. Par cette loi, la CNAMTS (Caisse Nationale d'Assurance Maladie des Travailleurs Salariés) a été chargée de gérer une base de donnée regroupant les données de remboursement des soins effectués en ambulatoire (de ville), ayant pour objectif de

[26] Ordonnance n° 96-345 du 24 avril 1996 relative à la maîtrise médicalisée des dépenses de soins.

[27] Dont l'ordonnance n° 96-50 du 24 janvier 1996 relative au remboursement de la dette sociale ; l'ordonnance n° 96-51 du 24 janvier 1996 relative aux mesures urgentes tendant au rétablissement de l'équilibre financier de la sécurité sociale, puis l'ordonnance n° 96-345 du 24 avril 1996 relative à la maîtrise médicalisée des dépenses de soins ; l'ordonnance n° 96-346 du 24 avril 1996 portant réforme de l'hospitalisation publique et privée.

contribuer à une meilleure gestion des politiques de santé, en contribuant à « la connaissance des dépenses de l'ensemble des régimes d'Assurance Maladie, à la définition, à la mise en œuvre et à l'évaluation des politiques de santé, à l'amélioration de la qualité des soins et à la transmission aux professionnels de santé des informations relatives à leur activité, à leurs recettes et, s'il y a lieu, à leurs prescriptions »[28].

En parallèle, depuis 1968, l'INSERM (Institut National de la Santé et de la Recherche Médicale) gère la Base de données sur les causes médicales de décès (BCMD) en France, qui permet de produire et d'analyser la statistique nationale des causes médicales de décès (statistique établie à partir des informations recueillies dans le certificat de décès), grâce à la centralisation de l'ensemble des décès survenus sur le territoire français.

Ces trois bases de données majeures comprennent donc les données dites « médico-administratives », issues des systèmes d'information hospitaliers, les données du système d'information de l'assurance maladie, les données sur les causes de décès, ainsi que certaines données de remboursement transmises par les organismes d'assurance maladie complémentaire. Il est envisagé d'y intégrer, d'ici 2020, les données relatives au handicap du système d'information commun des maisons départementales des personnes handicapées (SIMDPH).

Ces données sont anonymisés afin de garantir la protection de la vie privée des personnes concernées, mais permettent néanmoins de grandes avancées en matière de santé publique (prévention, gestion des risques sanitaires…) ou de pilotage du système de santé, ou encore en matière d'élaboration de politiques sanitaires et sociales (en permettant de déterminer l'évolution du reste à charge pour les patients…). En cela, ces bases de données gagnent pour beaucoup à être mises à la disposition de la communauté des chercheurs et des acteurs de la santé.

[28] Sur le site du SNDS : https://www.snds.gouv.fr/SNDS/Composantes-du-SNDS

Depuis 2016, ces trois bases stratégiques sont réunies, grâce à la loi dite « de modernisation de notre système de santé »[29], au sein du SNDS (Système National des Données de Santé), créant ainsi une des bases de données de santé les plus riches d'Europe : aujourd'hui, la France dispose des données de santé de plus de 67 millions de personnes, sur un historique de plus de 10 ans.

La loi[30] prévoyait l'ouverture de ces données de santé ainsi que la création d'un « Institut National des Données de Santé » (INDS), groupement d'intérêt public constitué entre l'Etat, des organismes assurant une représentation des malades et des usagers du système de santé, des producteurs de données de santé et des utilisateurs publics et privés de données de santé, y compris des organismes de recherche en santé.

Cet institut, aux termes du Code de la Santé Publique, est notamment chargé de « veiller à la qualité des données de santé et aux conditions générales de leur mise à disposition, garantissant leur sécurité et facilitant leur utilisation dans le respect de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés », de « faciliter la mise à disposition d'échantillons ou de jeux de données agrégées », dans le respect de recommandations de bonnes pratiques fixées par la CNIL, traduite notamment à travers des « méthodologies de référence » (MR) [31].

---

[29] Loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé.

[30] En un article 193, intégré au sein d'un « Chapitre V : Créer les conditions d'un accès ouvert aux données de santé ».

[31] A savoir, les méthodologies de référence « 004 », « 005 » et « 006 » :

- Délibération n° 2018-155 du 3 mai 2018 portant homologation de la méthodologie de référence relative aux traitements de données à caractère personnel mis en œuvre dans le cadre des recherches n'impliquant pas la personne humaine, des études et évaluations dans le domaine de la santé (MR-004) ;
- Délibération n° 2018-256 du 7 juin 2018 portant homologation d'une méthodologie de référence relative aux traitements de données nécessitant l'accès par des établissements de santé et des fédérations aux données du PMSI et des résumés de passage aux urgences (RPU) centralisées et mises à disposition sur la plateforme sécurisée de l'ATIH (MR 005) ;
- Délibération n° 2018-257 du 7 juin 2018 portant homologation d'une méthodologie de référence relative aux traitements de données nécessitant l'accès pour le compte des personnes produisant ou commercialisant des produits mentionnés au II de l'article L. 5311-1 du code de la santé publique aux données du PMSI centralisées et mises à disposition par l'ATIH par l'intermédiaire d'une solution sécurisée (MR 006).

D'autres sources de données, de tailles, d'importance, d'intérêt et de maturité variables, existent également. On compte ainsi près de 260 bases de données de santé publiques (le portail Epidémiologie-France recense même jusqu'à 500 bases de données médico-économiques, cohortes, registres et études en cours)[32]. De façon non-exhaustive, nous pouvons ainsi citer les différentes bases de données issues de la recherche et de cohortes nationales ou locales, les données d'hospitalisation et le dossier patient informatisé (DPI, qui peut être hospitalier, propre à un établissement, ou de GHT), les données génomiques, les données issues du « nouveau » Dossier Médical Partagé[33], etc.

A la différence des données du SNDS, ces bases contiennent des données dites « cliniques » (issues du soin ou de la recherche). Leur qualité est néanmoins très variable, selon que la base ait été structurée, traitée, nettoyée, mise à jour, fusionnée ou encore enrichie.

Malgré les différents efforts en matière de collecte et de centralisation des données, celles-ci constituent aujourd'hui un patrimoine très fragmenté, dispersé, et bien que leur production ne cesse de croître, leur partage et leur exploitation restent insuffisants[34].

Face à ce constat et afin de révéler pleinement tout le potentiel des données de santé en permettant leur traitement et leur exploitation, une régulation a donc été opérée par le pouvoir politique, à travers différentes réformes et l'organisation de groupes de travail à l'échelle nationale ayant notamment pour objet de définir des standards de structuration, de codage et d'intégration

---

[32] « Big data en santé : des défis techniques, humains et éthiques à relever », INSERM, 1er Juillet 2016.

Consulté le 06/06/19 : https://www.inserm.fr/information-en-sante/dossiers-information/big-data-en-sante

[33] Le dossier médical partagé (ou personnel, avant 2015), est un projet public lancé dès 2004 (par la loi n°2004-810 du 13 Août 2004 relative à l'Assurance maladie) en France et visant à fournir à chaque usager du système de santé français un dossier médical numérique, informatisé, contenant toutes ses données médicales, ainsi que d'autres données diverses liées à la santé.

[34] Cour des Comptes, « Les données personnelles de santé gérées par l'assurance maladie - une utilisation à développer, une sécurité à renforcer », communication à la commission des affaires sociales et à la mission d'évaluation et de contrôle des lois de financement de la sécurité sociale de l'Assemblée nationale, mars 2016.

des données et de mettre en commun ces différentes bases au sein de nouvelles bases de données centralisées, d'entrepôts de données de santé, de plateformes de données de santé.

C'est ainsi qu'en France, depuis quelques années, des entrepôts de données de santé se sont constitués au sein de différentes établissements de santé publics comme privés (notamment des CHU : AP-HP ; HCL ; CHU de Lyon, de Bordeaux, de Rennes, de Montpellier, de Lille…). Les Entrepôts de Données de Santé (EDS) sont des outils informatiques permettant la collection, l'intégration puis le traitement des données de santé provenant d'un grand nombre de sources d'information clinique (dossier patient informatisé, système d'information des laboratoires et d'imagerie, prescription informatisée, dossier infirmier…).

C'est afin d'organiser ce réseau de bases de données de santé (médico-administratives et cliniques) que la loi de réforme du système de santé, actuellement en discussion au Parlement[35], envisage d'une part de créer une « Plateforme de données de santé » (Health Data Hub), sous forme de groupement d'intérêt public (GIP), qui serait chargé des missions de l'INDS, auxquelles s'ajouteraient d'autres prérogatives et missions. Ainsi, le « Health Data Hub » se voit fixés pour objectifs de favoriser l'utilisation et de multiplier les possibilités d'exploitation des données de santé, en particulier dans les domaines de la recherche, de l'appui au personnel de santé, du pilotage du système de santé, du suivi et de l'information des patients ; de permettre le développement de nouvelles techniques, notamment celles liées aux méthodes d'intelligence artificielle ; ou encore de promouvoir l'innovation dans l'utilisation des données de santé.

La volonté des pouvoirs publics de promouvoir l'accès, l'utilisation et l'exploitation des données de santé semble apparaitre de manière évidente. Néanmoins, cette ouverture ne constitue pas une

[35] Projet de loi relatif à l'organisation et à la transformation du système de santé, dans le cadre du plan « Ma Santé 2022 ».

évidence juridique, éthique ou économique, notamment dans le cadre du service public hospitalier. Il convient en effet de mettre en balance l'encadrement juridique actuel des données de santé et les intérêts majeurs d'un partage plus large de ces données.

B. Données de santé et Service Public Hospitalier : une ouverture sujette à controverse.

Les principes du service public, formulé par Louis ROLLAND[36], constituent des obligations imposées, par principe et selon des valeurs reconnues comme fondamentales, aux différentes services publics. Trois principes de bases s'appliquent ainsi aux services publics : celui de continuité, celui d'égalité et celui de mutabilité. Ces principes de bases, déclinés selon les besoins et les situations, appliqués par la jurisprudence[37], seront ainsi développés et spécialisés pour le domaine de l'hôpital, allant jusqu'à former les principes du service public hospitalier.

Au cours des années 1970, la notion de service public hospitalier voyait le jour[38] à travers la loi Boulin du 31 décembre 1970. Le service public hospitalier est alors défini par ses missions, lesquelles doivent être accomplies dans le respect des principes du service public (continuité, égalité,

---

[36] ROLLAND Louis, « *Précis de droit administratif*, » petit précis Dalloz, 1947, 9ème édition, p.16.

[37] Notamment :

Pour le principe de continuité : Conseil d'Etat, 7 Août 1909, Winkell et Conseil d'Etat, 7 Juillet 1950, Dehaene.

Pour le principe d'égalité devant le service public : Conseil d'Etat, 9 Mars 1951, Société des Concerts du Conservatoire et Conseil d'Etat, 10 Mai 1974, Denoyez et Chorques.

Pour le principe de mutabilité : Conseil d'Etat, 27 Janvier 1961, Vannier.

[38] Loi Boulin du 31 Décembre 1970

mutabilité). Au départ relativement assez réduites (soins aux malades, blessés et femmes enceintes, et pour les établissements participant au service public hospitalier, l'enseignement, la recherche et la prévention), les activités des établissements d'hospitalisation se sont développées, le législateur rajoutant à chaque réforme de nouvelles missions propres au service public hospitalier.

La notion, disparue en 2009, réapparue en 2016[39], apparait désormais comme constituée d'obligations, autant de missions qui s'imposent aux établissements publics comme privés qui l'assurent[40]. Ces obligations sont mentionnées à l'article L6111-1 du Code de la Santé Publique[41] (CSP). Ces missions doivent donc être exercées, selon l'article L 6112-1 du CSP, « dans le respect des principes d'égalité d'accès et de prise en charge, de continuité, d'adaptation et de neutralité et conformément aux obligations définies à l'article L. 6112-2 ».

Mais, d'après Sabine BOUSSARD, « l'hôpital public ne peut pas avoir le monopole du service public hospitalier. Il ne faut pas perdre de vue que l'activité de soin est une activité économique au sens du droit européen. Le service public hospitalier relève de la catégorie des services d'intérêt

---

[39] Loi n°2016-41 du 26 Janvier 2016 de modernisation de notre système de santé.

[40] V. VIOUJAS, « *La résurrection du service public hospitalier* », AJDA, 2016, p1272.

[41] « Les établissements de santé publics, privés d'intérêt collectif et privés assurent, dans les conditions prévues au présent code, en tenant compte de la singularité et des aspects psychologiques des personnes, le diagnostic, la surveillance et le traitement des malades, des blessés et des femmes enceintes et mènent des actions de prévention et d'éducation à la santé.

Ils délivrent les soins, le cas échéant palliatifs, avec ou sans hébergement, sous forme ambulatoire ou à domicile, le domicile pouvant s'entendre du lieu de résidence ou d'un établissement avec hébergement relevant du code de l'action sociale et des familles.

Ils participent à la coordination des soins en relation avec les membres des professions de santé exerçant en pratique de ville et les établissements et services médico-sociaux, dans le cadre défini par l'agence régionale de santé en concertation avec les conseils départementaux pour les compétences qui les concernent.

Ils participent à la mise en œuvre de la politique de santé et des dispositifs de vigilance destinés à garantir la sécurité sanitaire.

Ils mènent, en leur sein, une réflexion sur l'éthique liée à l'accueil et la prise en charge médicale.

Ils peuvent participer à la formation, à l'enseignement universitaire et postuniversitaire, à la recherche et à l'innovation en santé. Ils peuvent également participer au développement professionnel continu des professionnels de santé et du personnel paramédical ».

économique général du droit européen de la concurrence. Le caractère économique de l'activité entraîne des contraintes du point de vue du financement du service public hospitalier »[42].

La nature même du SPH est donc source de discussion, car elle est double, à la fois désintéressée par essence et intéressée par sa pratique. Ainsi, le législateur a dû réfléchir à cette nature complexe : l'article L 6141-1 du CSP dispose que « les établissements publics de santé sont des personnes morales de droit public dotées de l'autonomie administrative et financière. Ils sont soumis au contrôle de l'Etat dans les conditions prévues par le présent titre. Leur objet principal n'est ni industriel ni commercial […] ». Cette définition par formulation négative indique en réalité la lutte actuelle qui existe entre une privatisation, au moins partielle, du SPH, et son maintien dans le giron public. La première solution serait en effet justifiée par les différentes réformes étudiée précédemment, qui ont introduit au sein du SPH des modalités de financement (T2A), des modalités d'organisation et de fonctionnement (directeur renforcé, directoire, conseil de surveillance), des modalités de gestion (*lean management*…) issues du secteur privé.

Néanmoins, si les méthodes et techniques issues du secteur privé sont transposables au service public hospitalier, le caractère commercial, induisant la préférence exclusive pour la rentabilité, ne saurait sûrement pas s'accommoder au SPH, lequel repose sur des principes différents, issus des principes du service public, et sur des valeurs de bénéfice commun (volonté d'amélioration de la santé de la population, préférence pour l'utilité sanitaire et sociale, etc…), et non pas privé.

Face à ce constat, il apparait donc que la notion de service public hospitalier est évolutive et source de nombreux débats, et le caractère économique de ses activités interroge. C'est dans ce cadre que

[42] BOUSSARD S., « *Les vicissitudes du service public hospitalier* », RFDA 2016, p. 565.

prennent place les réflexions au sujet de l'ouverture des données de santé, de leur protection et de leur valorisation.

En effet, les données de santé produites par les hôpitaux peuvent, sous certains aspects, être considérées comme des données publiques, en ce qu'elles sont produites ou collectées par un établissement public dans le cadre de ses activités de service public. Elles font, en conséquence, partie du patrimoine immatériel public, au même titre que le patrimoine audiovisuel, les marques, les savoir-faire. Cet ensemble constitue un patrimoine dont la valorisation peut, d'une part, servir les objectifs stratégiques des administrations, et d'autre part, lorsqu'il est partagé avec des tiers, moderniser la société au service du citoyen. La mobilisation des données de santé constitue, en effet, un levier très puissant de transformation positive de notre système de santé.

Néanmoins, selon le principe d'open data, ces données devraient, en principe, être publiées ou tenues à la disposition du public, citoyens comme entreprises : l'accessibilité de la donnée publique (qui implique aussi la liberté d'accès aux documents administratifs) est un des éléments de la transparence d'une gouvernance, considérée comme faisant partie de la « troisième génération des droits de l'Homme »[43]. Ce mouvement visant à rendre accessible à tous via le web les données publiques collectées par des organismes publics connait cependant des exceptions : sont exclues de l'ouverture des données publiques les données relevant de la vie privée (certaines données présentent un caractère personnel, des informations sur des personnes, le droit peut alors prévoir leur confidentialité), relevant de la sécurité nationale ou lorsque des tiers détiennent des droits de propriété intellectuelle sur tout ou partie de ces informations et données.

[43] BRAIBANT Guy, « Droit d'accès et droit à l'information », Mélanges Robert-Edouard Charlier, Ed. de l'Université, 1981, p. 703.

Deux aspects peuvent ainsi être identifiés afin d'assurer l'accès aux données de santé, de soutenir la recherche et l'innovation tout en renforçant la confiance que les usagers placent dans les différentes acteurs de la santé (hôpitaux, industriels, professionnels de santé, chercheurs, administrations publiques…) : la protection et la valorisation des données de santé.

D'une part, il s'agit de protéger les données, afin d'obtenir, par la preuve du caractère vertueux et respectueux des droits de l'usage des données, la confiance des usagers en tant que « créateurs » de données. Ces outils, sous l'angle juridique, sont notamment issus des textes nationaux et internationaux en matière de protection des données, à savoir notamment le Règlement Européen relatif à la protection des données (RGPD) et la loi Informatique et Liberté (LIL).

D'autre part, il s'agit de valoriser les données, à l'aide des différents outils juridiques existant. Ces outils induisent souvent une protection préalable de l'objet de la valorisation, et ont pour objectif de valoriser les actifs immatériels utilisés ou développés par les hôpitaux. Ils consistent notamment en différents outils de propriété intellectuelle, déjà existants ou en réflexion, et sont notamment contenus dans le Code de la Propriété Intellectuelle (CPI). Néanmoins, d'autres outils de valorisation ou liés à la valorisation existent et sont présents au sein du Code de la Santé Publique (CSP), du Code de la Recherche (CR) ou encore du Code des Relations entre le Public et l'Administration (CRPA). En cela, la protection et la valorisation des données de santé sont indissociables. La valorisation des données de santé requiert, au surplus, une réflexion stratégique relative aux modèles économiques, aux organisations, à l'éthique relatifs à sa mise en œuvre.

L'ouverture des données de santé prend donc place au sein d'un corpus juridique étoffé et complexe, entre protection et valorisation de ces données.

Cependant, face à cette volonté d'ouverture des données traduite par le droit, des questions juridiques, économiques, éthiques et déontologiques se posent : comment mettre en œuvre un

processus de valorisation économique du recours aux données de santé à la fois performant, efficient et respectueux du cadre juridique et de principes éthiques ?

Du point de vue juridique :

La protection juridique des données personnelles de santé est-elle suffisante ? Est-elle trop importante ? La protection juridique des bases de données est-elle suffisante ? Qui possède un droit de propriété sur les bases de données et les données qu'elles contiennent ?

Valoriser les données est-il une mission du service public hospitalier ? La valorisation des données de santé peut-elle aboutir à la réalisation d'un bénéfice ou doit-elle se borner à une valorisation « au juste prix », équivalente au prix de revient ? Comment intégrer la valorisation dans le respect des règles du droit public économique, du droit de la concurrence ? Comment articuler la valorisation des données, les droits des patients, le droit des données personnelles et l'éthique médicale ?

Du point de vue économique :

Quel modèle économique peut-on envisager pour la valorisation des données de santé ? Quelle valeur attribuer aux données de santé ? Faut-il se fonder sur le prix de revient, et si oui, quels coûts prendre en compte ? Faut-il se fonder sur le prix de marché, la valeur d'usage, la valeur économique de la prestation pour le bénéficiaire ?

Du point de vue éthique et déontologique :

Qu'en est-il du secret médical ? Des droits de l'usager vis-à-vis des données le concernant (consentement au recueil, à l'utilisation, droit d'opposition…) ? Quel avenir pour les professions médicales à l'ère de l'IA ? Quelle valeur affecter à une ou plusieurs données ? Valoriser les données est-il éthique ? Comment concilier les perspectives de progrès avec les aspirations humaines, morales de notre société ?

Il s'agit en effet de déployer les solutions numériques en santé dans le respect des principes éthiques qui fondent notre société, en assurant la protection de la vie privée, en garantissant une exigence forte de qualité dans la collecte et l'utilisation des données, afin de répondre aux

dysfonctionnements du système de soins et de contribuer à un égal accès à des soins de qualité pour tous, tout en amélioration l'efficacité et l'efficience du service public hospitalier, au bénéfice de la santé des usagers du système de santé (prévention, diagnostic et soins, notamment dans un contexte d'augmentation des maladies chroniques et de la dépendance).

Problématique

Tout au long de ce travail de recherche, nous allons donc tenter de répondre à la question suivante :

Comment concilier protection et valorisation des données de santé au sein du service public hospitalier ?

Nous verrons, premièrement, que la protection des données de santé est non seulement nécessaire à la valorisation (afin d'obtenir la confiance des usagers et de pouvoir développer des technologies d'IA, mais également afin de protéger les bases de données par des outils juridiques) mais également bien réelle (Partie 1). Nous verrons ensuite que la valorisation, bien qu'elle soit éminemment souhaitable, est un sujet particulièrement complexe à appréhender, entre certitudes et incertitudes (Partie 2).

Partie I : La protection des données de santé

De plus en plus de données sont accumulées du fait de l'important développement et du large déploiement des technologies numériques. Parmi ces données, les « données personnelles », dont certaines sont « sensibles », comme les données de santé ou les données biométriques, attirent de nombreuses convoitises de la part d'acteurs très divers (industriels de santé, chercheurs académiques, industriels du numérique…) du fait des applications prometteuses qu'elles laissent envisager.

En particulier, les cinq géants du web (les « GAFAM », pour Google, Amazon, Facebook, Apple et Microsoft) qui réunissent aujourd'hui près de 80% des données personnelles mondiales[44], ou encore les Data Brokers (entreprises obtenant ou rachetant des données et les commercialisant à prix d'or) souhaiteraient pouvoir entrer en possession de données massives de santé, lesquelles sont en partie détenues d'une part par des professionnels et des établissements de santé (données collectées dans le cadre du soin, d'une prise en charge médicale), d'autre part par utilisateurs d'applications recueillant des données primaires pouvant être croisées avec d'autres données et permettant de créer une information concernant la santé.

Néanmoins, ouvrir l'accès à ces données sensibles à certains acteurs, notamment ceux mentionnés plus tôt, ne fait pas l'objet d'un consensus évident. En effet, de nombreuses craintes, plus ou moins fondées, font état des potentielles dérives de l'usage de ces données sensibles, allant à l'encontre des droits des personnes concernées ou amenant à une aliénation, une dépossession des individus de leurs données et du contrôle qu'ils en ont.

Aussi, de nouvelles réflexions ont été menées sur la protection des données de santé, leur contrôle, les risques pour la vie privée et la liberté des individus. Le droit est ensuite venu encadrer

---

[44] HURIET Claude, in « Innovations en santé publique, des données personnelles aux données massives (Big data) – Aspects cliniques, juridiques et éthiques », *Dalloz*, Thèmes et commentaires, Ethique biomédicale et normes juridiques, 2018.

les pratiques d'accès aux données ainsi que leur exploitation, et a rapidement été suivi par des mesures techniques et organisationnelles adaptées afin d'assurer le respect du cadre juridique instauré.

D'autre part, l'accès et l'exploitation des données ayant été autorisé, légitimé par le droit, les préoccupations au sujet de la valorisation des données ont bientôt dépassé le simple enjeu juridique de la pratique pour rapidement devenir un enjeu économique.

Cet aspect économique de la valorisation des données de santé a donc dû être appréhendé de nouveau par le droit, afin d'encadrer les pratiques et d'assurer, cette fois, le respect de la propriété privée, de la propriété intellectuelle, tout en la conciliant avec le principe d'intérêt général ou public[45].

En effet, notamment depuis la révolution Française, les atteintes à la propriété privée ont été progressivement encadrées, précisées, dans le droit français, notamment à travers une jurisprudence abondante sur ce sujet. Il a ainsi été considéré que les atteintes au droit de propriété pouvaient être justifiées par des considérations d'intérêt général, sous la condition que soit établi et respecté un bilan coût/avantage au préalable[46].

Cependant, le développement d'un droit communautaire à l'échelle de l'Union Européenne a modifié l'ordonnancement juridique national, notamment le droit public économique fixant les règles liées à concurrence.

---

[45] Les deux notions, bien que proches, sont à distinguer. La notion d'intérêt général est plutôt utilisée dans le droit français, tandis que la notion d'intérêt public est plutôt usitée en droit européen. Néanmoins, les deux notions seront, dans ce mémoire, considérées comme équivalentes.

[46] CE, 1971, *Ville Nouvelle Est* et CE Ass., 1972, *Ste Marie de l'Assomption.*

Ainsi, si l'intérêt général est mentionné dans plusieurs articles du traité de Rome[47] (Traité instituant la « Communauté Economique Européenne », puis la « Communauté Européenne », jusqu'en 2007, avec la signature du « Traité sur le Fonctionnement de l'Union Européenne ») en sa version « TCE » successive au Traité de Maastricht – article 16, article 86, article 90 – ainsi qu'au sein de la Charte des Droits Fondamentaux de l'Union Européenne[48], il résulte des divers textes européens un resserrement de la notion d'intérêt général, laquelle doit se concilier avec le marché et la liberté d'entreprise, la libre concurrence, etc.

Ce resserrement de la notion s'est également appliqué, par transposition, sur le droit français, et par voie de conséquence, sur sa jurisprudence. *De facto*, le cadre juridique relatif à la valorisation des données se doit aujourd'hui de concilier avec subtilité les droits de la propriété – intellectuelle dans le cas des données –, avec l'intérêt général.

Néanmoins, de nos jours, avec l'avènement des nouvelles technologies numériques d'information et de communication (NTIC), ou encore de la blockchain (technologie de stockage et de transmission d'informations, transparente, sécurisée, et fonctionnant sans organe central de contrôle[49], définie par le mathématicien Jean-Paul Delahaye, comme « un très grand cahier, que tout le monde peut lire librement et gratuitement, sur lequel tout le monde peut écrire, mais qui est impossible à effacer et indestructible.»[50]), avec les nouvelles possibilités que ces outils permettent

---

[47] Traité instituant la Communauté économique européenne (TCEE), signé le 25 mars 1957, puis la « Communauté Européenne », depuis 1992 (Traité de Maastricht) jusqu'en 2007, avec la signature du « Traité sur le Fonctionnement de l'Union Européenne », également appelé traité de Rome.

[48] Charte des droits fondamentaux de l'Union européenne, 7 Décembre 2000 : « L'Union reconnaît et respecte l'accès aux services d'intérêt économique général tel qu'il est prévu par les législations et pratiques nationales, conformément au traité instituant la Communauté européenne, afin de promouvoir la cohésion sociale et territoriale de l'Union ».

[49] https://blockchainfrance.net/decouvrir-la-blockchain/c-est-quoi-la-blockchain/

[50] DELAHAYE Jean-Paul, « Les blockchains, clefs d'un nouveau monde », *Pour la Science* - n° 449, pp. 80-85 - Mars 2015.

(étude, stockage, traitement, réception ou émission d'informations), la question de la propriété est sujette à discussions.

En effet, à l'heure où les patients, usagers du système de santé, peuvent contrôler leurs données et l'usage qui en est fait, un nouveau droit, une nouvelle forme de « propriété intellectuelle » semble apparaitre : une forme de propriété des patients sur leurs données.

Il s'agira donc, dans un premier temps, d'étudier les droits des usagers sur leurs données de santé, leur origine ainsi que la manière dont leur protection est mise en œuvre (Titre 1), pour ensuite étudier les fondements, limites et critiques relatives aux droits de propriété relatifs aux bases de données de santé (Titre 2).

Titre 1 : La protection individuelle des données de santé : les droits des personnes concernées

Les données de santé, considérées de manière individuelle (« la donnée de santé ») ont fait l'objet, récemment, de réflexions éthiques et juridiques d'importance. En effet, après la survenance de certains scandales (Cambridge Analytica[51], ventes de dossiers médicaux sur le Dark Web, incidents relatifs à des fuites de données constatés dans le secteur de la santé…), il s'agissait de prendre du recul et de réfléchir à ce que la société française tolérait ou non en matière d'usage de ses données, et plus spécifiquement en matière d'usage de ses données de santé.

Ainsi, un corpus de normes éthiques liées aux données de santé a pu être élaboré, puis traduit juridiquement à travers des textes à la fois européens et nationaux. Ces textes constituent ainsi une somme des volontés et des revendications de la société en matière de protection de la vie privée et d'utilisation des données de santé, données particulièrement sensibles du fait de leur caractère intime et des nuisances spécifiques qu'un usage malveillant pourrait provoquer.

Il s'agit en effet d'opérer une conciliation entre ce qu'il est techniquement possible de faire et ce que la société souhaite tolérer – ou non.

Ces normes sont donc venues encadrer les pratiques, d'une part en matière de recueil des données (information et consentement des personnes concernées) (Chapitre 1), d'autre part en matière d'utilisation et de réutilisation des données (Chapitre 2).

[51] Les données du réseau social Facebook ont été exploitées illégalement pour influencer les élections présidentielles américaines de 2016. Ce même réseau social sera à l'origine d'un autre scandale lorsqu'une enquête parvint à démontrer que Facebook avait contacté des hôpitaux afin de tenter de collecter les données de santé de leurs patients pour les associer avec leurs comptes sur le réseau social.

Chapitre 1 : Une protection indispensable

Section 1 : La protection de la donnée de santé, une nécessité éthique

Face au développement de l'usage des big data en santé, les citoyens expriment déjà des craintes et des appréhensions liées au potentiels usages malveillants de leurs données de santé.

Face à ces craintes, de nombreuses réflexions éthiques ont été menées par des acteurs très divers : le Conseil National de l'Ordre des Médecins (CNOM), qui faisait paraitre en janvier 2018 un « Livre Blanc sur le médecin et le patient dans le monde des data, des algorithmes et de l'intelligence artificielle », le Comité Consultatif National d'Ethique (CCNE), qui faisait paraitre deux avis en Septembre 2018 (avis 129[52]) et en Mai 2019 (avis 130), portant respectivement sur la révision de la loi de bioéthique et comportant une thématique « Numérique et Santé » et sur les données massives (big data) en santé[53], ou encore des chercheurs et acteurs académiques, universitaires ou professionnels, qui ont réalisé des sur le sujet[54]…

Ces divers travaux ont permis d'identifier différents points de vue concernant les nouvelles technologies numériques, d'information et de communication (le numérique étant considéré en tant que science et technologie du traitement de l'information), ainsi que de nombreuses attentes

---

52 Avis 129 du CCNE, « Contribution du Comité consultatif national d'éthique à la révision de la loi de bioéthique 2018-2019 », adopté le 18 septembre 2018.

53 Avis 130 du CCNE sur « Données massives (big data) et santé : une nouvelle approche des enjeux éthiques », paru le 28 mai 2019.

54 BERANGER Jérôme, « La valeur éthique de la donnée de santé à caractère personnel : vers un nouveau paradigme de l'écosystème médical dématérialisé », Sciences de la société, 95 / 2016.

HERVE Christian, STANTON-JEAN Michèle (dir.), « Innovations en santé publique, des données personnelles aux données massives (Big data) – Aspects cliniques, juridiques et éthiques », Dalloz, Thèmes et commentaires, Ethique biomédicale et normes juridiques, 2018.

HERVE Christian, STANTON-JEAN Michèle, MARTINENT Eric (dir.), « Les systèmes informatisés complexes en santé – Banque de données, télémédecine : normes et enjeux éthiques », Dalloz, Thèmes et commentaires, Actes, 2013

et revendications éthiques, dont l'importance de la protection des données, fondement de la confiance des citoyens envers les différents traitements de leurs données.

Le CCNE, dans son avis 129, commence ainsi par constater le caractère inévitable des apports technologiques du numérique, notamment dans le domaine de la santé. Il en rappelle ensuite les avantages (amélioration de la santé, rationalisation des coûts…), ainsi que l'aspect très humain de ces technologies, le traitement de l'information étant « au cœur de l'humain ». Il affirme, ensuite, que « le numérique est […] fondamentalement au cœur même de l'ensemble du système de santé ». Néanmoins, le CCNE souligne également le risque d'une déshumanisation de la relation soignant/soigné, corolaire de l'avènement des technologies numériques, ainsi que les risques et craintes liés à l'utilisation frauduleuse ou abusive des données de santé.

Cet avis a ensuite servi d'impulsion au CCNE pour qu'il s'engage plus profondément dans une réflexion éthique relative au domaine du numérique et de la santé. Cette impulsion a abouti à la rédaction d'un nouvel avis, numéro 130, sur la thématique « données massives et santé ».

Le Comité, de même que le CNOM dans son livre blanc paru un an auparavant, estime ainsi que les grands principes de l'éthique médicale (respect de la personne et de son autonomie, justice, pertinence, bienfaisance et non-nuisance) doivent être appliqués avec d'autant plus d'attention dans un contexte où les innovations technologiques évoluent rapidement, portées par des acteurs divers, dans des situations de recueil et de traitement tout aussi diverses.

En effet, le comité rappelle que « la réflexion éthique doit prendre en compte le fait que certaines innovations peuvent ne pas avoir pour finalité le soin, mais l'exploitation d'un marché se présentant comme relevant du bien-être », et rappelle, de plus, que « toute donnée primaire issue d'une activité humaine – même sans lien apparent avec la santé, peut contribuer – par son croisement avec d'autres données qui ne lui sont pas liées – à la création d'une information nouvelle relative à la santé d'une personne ».

Nous pourrions également rajouter que ces données peuvent intéresser des industriels, qui y voient par exemple un moyen de mieux gérer les risques liés à leurs produits ou encore un outil permettant de mettre en place des moyens correspondant aux besoins, afin d'accroître *in fine* leur chiffre d'affaire. Il s'agit ainsi de différencier plusieurs situations d'usage des données : au-delà des situations orientées vers le public, le patient – dans le cadre du soin ; de la recherche ; de la gestion des soins ; dans le cadre de la vie personnelle enfin –, se trouvent des situations ayant un objectif commercial, porté vers la recherche ou la maximisation d'un profit – marketing, profilage, identification d'un marché favorable pour la conception d'un nouveau médicament, amélioration de la performance économique…

Aussi, ces différentes situations mettent-elles en cause la protection de la vie privée et peuvent-elles aboutir à la stigmatisation de personnes ou de groupes, et menacer non-seulement la vie privée, mais également les principes de solidarité et d'équité, qui fondent notre le système de santé : soin et commerce apparaissent comme étant à la fois inconciliables et de plus en plus complexes à distinguer nettement, dans notre société actuelle, du fait du développement des technologies numériques et de l'usage des données qui découle.

C'est pour cette raison majeure que la protection des données de santé apparait comme une nécessité éthique : il s'agit d'affirmer, de réaffirmer les principes éthiques sans lesquels la protection des droits fondamentaux de la personne ne pourrait être assurée, dans un contexte d'innovation, de possibilités et de risques inhérents à ce contexte de mutation.

Section 2 : La protection de la donnée de santé : d'une nécessité stratégique à la nécessité d'une stratégie

Au-delà de la nécessité éthique de protéger la donnée de santé, indispensable afin d'obtenir la confiance des citoyens, il s'agit également de déterminer la stratégie la plus pertinente afin de faire respecter cette exigence éthique. En effet, derrière cette volonté se trouve de nombreuses modalités de mise en œuvre, impliquant également des réflexions éthiques : au-delà de l'exigence éthique de protection des droits de la personne face aux risques de dérives, il s'agit également de respecter la liberté individuelle sans pour autant compromettre la solidarité et l'intérêt collectif, indispensables à l'acquisition de nouvelles connaissances et au à l'innovation en santé basés sur le recours aux données massives de santé.

Premièrement, afin de protéger les droits fondamentaux de la personne, notamment le droit au respect de la vie privée, dans le cadre du recueil et du traitement des données de santé, il importe d'exiger comme fondement le consentement libre et éclairé de la personne concernée, lequel repose sur une obligation d'information.

Cette information peut revêtir différents caractères. Ainsi, entendue au sens du droit des contrats, l'information qui doit être transmise doit être d'une importance « déterminante » pour la conclusion du contrat, dès lors que, légitimement, la personne concernée « ignore cette information ou fait confiance au responsable de traitement »[55]. Le code civil continue en indiquant que « ont une importance déterminante les informations qui ont un lien direct et nécessaire avec le contenu du contrat ou la qualité des parties. » Pour autant, l'information ne doit pas être excessive afin de ne pas « noyer » la personne concernée par les données[56]. Inversement, lorsque la personne concernée,

[55] Article L1112-1 du Code civil.

[56] Cass 1re, 18 oct. 1994

comme c'est souvent le cas, ne dispose pas de l'information nécessaire à la formation d'un consentement libre et éclairé du fait de son impossibilité d'accéder à l'information (information indisponible ou n'étant pas connue du grand public, du fait de son caractère technique par exemple) ou lorsqu'elle porte une confiance légitime envers le responsable de traitement, alors l'obligation de loyauté de celui-ci se voit renforcée.

Entendue au sens du droit de la santé, la qualité l'information concernant les données de santé peut également être rapprochée de la qualité de l'information médicale, laquelle doit, selon l'article 35 du Code de déontologie médicale être « loyale, claire et appropriée ».

Ce consentement est néanmoins malmené par les conditions mêmes de recueil et d'exploitation des données massives : les finalités d'exploitation sont parfois incertaines, ou font l'objet d'une modification ; le processus d'analyse des données est souvent complexe et difficilement compréhensible ou accessible au grand public ; en conséquence l'information délivrée lors du recueil du consentement est parfois imprécise. Il apparait néanmoins difficilement acceptable, éthiquement, de freiner l'acquisition de connaissances ou le développement des innovations en santé sur le fondement d'une information imparfaite.

Aussi, il apparait indispensable, outre d'informer la personne, de définir une modalité d'information adaptée à cet objet spécifique que constituent les données massives en santé. Il s'agit alors de réaffirmer et de redéfinir les modalités de protection de la personne, tout au long du processus impliquant la mobilisation de données massives de santé. Il ne s'agit donc plus de protéger la personne uniquement en amont, mais également, et surtout, en aval, à travers différentes garanties et protections.

Cette protection de la personne et de ses droits peut se traduire à travers différents dispositifs.

Tout d'abord, l'éthique exige, de la part des responsables de traitement, une loyauté et une responsabilisation certaine. Elle leur impose ainsi une transparence de leurs processus et le devoir d'autoriser le contrôle, l'évaluation de leur accès aux données et des usages qu'ils en ont, ainsi que de leur déontologie.

Ce contrôle, dont la réalisation et l'élaboration des outils d'évaluation nécessaires se veut périodique du fait de l'évolutivité du domaine, repose en partie sur l'existence d'une institution de contrôle, une gouvernance identifiée, légitime et stable.

Cette exigence d'une gouvernance solide pose également la question de la souveraineté sur les données de santé. Celle-là, comme l'expriment de nombreux travaux[57], gagnerait à être assurée à un niveau élevé – au niveau national ou européen. Si mises en place au niveau national, des mutualisations et des échanges entre les institutions serait également souhaitable. La définition de modalités communes d'ouverture des données permettrait en effet à la France et à l'Europe de préserver une autonomie stratégique et de ne pas perdre l'opportunité et la richesse que constituent les données de santé pour le soin, la recherche et l'innovation en santé.

De plus, si l'information délivrée se doit d'être loyale et précise, elle doit également être adaptée à l'individu bénéficiaire de l'information ainsi qu'au contexte d'utilisation. Elle doit en outre

---

[57] Par exemple :

- Avis 130 du CCNE sur « Données massives (big data) et santé : une nouvelle approche des enjeux éthiques », paru le 28 mai 2019 ;
- VILLANI Cédric, LONGUET Gérard, « Rapport au nom de l'Office Parlementaire d'Evaluation des Choix Scientifiques et Technologiques sur l'Intelligence Artificielle et les Données de Santé », OPECST, 21 mars 2019 ;
- BRAIBANT Guy, « Données personnelles et société de l'information – Rapport au Premier Ministre sur la transposition en droit français de la directive n°95/46 », 3 mars 1998.

être aisément accessible, notamment aux personnes vulnérables, afin que ces personnes puissent faire valoir pleinement leurs droits.

Afin de garantir que cette information soit correctement reçue, le CCNE estime que « tous nos concitoyens doivent être sensibilisés aux spécificités des technologies numériques et aux avancées et risques qui leurs sont associés […] afin qu'ils puissent faire un usage responsable de leurs données personnelles. »

Enfin, afin de garantir les droits de la personne tout au long du processus de traitement de la donnée de santé, il s'agit également de déterminer des exigences éthiques relatives aux modalités de traitement et aux finalités du traitement de la donnée.

Afin de faire respecter les principes éthiques de non-nuisance et de bienfaisance, la confidentialité des données (le respect du secret médical le cas échéant), et donc, implicitement, leur sécurité, doit ainsi être garantie, de même que leur qualité. La finalité du traitement doit également être acceptée par la communauté. Classiquement, l'usage des données de santé est orienté vers quatre aspects de la médecine : le soin, la recherche, la prévention et les politiques de santé publique.

Dans le cadre de la recherche en santé, qui nous intéresse particulièrement, il importe notamment de trouver un équilibre entre une sous-exploitation des données, limitant en conséquence les recherches menées dans l'intérêt général, et un partage des données trop large, insuffisamment contrôlé (envers des acteurs industriels notamment), qui mettrait en cause les droits fondamentaux de la personne. L'intérêt général doit être recherché, et les principes éthiques doivent être appliqués de manière adaptée à chaque intervenant, à chaque chercheur selon sa discipline.

Chapitre 2 : Une protection effective

Les exigences éthiques indispensables à la protection des droits de la personne, afin de créer les conditions nécessaires à l'existence d'une confiance entre la personne concernée et le responsable de traitement, applicables à la collecte et à l'exploitation de la donnée de santé, ont été traduites à travers plusieurs textes juridiques, de nature et de portée variables.

La France a été le premier pays européen à se doter d'une législation spécifique en matière de protection des « données à caractère personnel », avec la loi du 6 janvier 1978 (loi dite « informatique et liberté ») [58]. Le cadre légal a ainsi longtemps été considéré comme solide et particulièrement protecteur des individus. Cependant, il a évolué afin de correspondre aux évolutions numériques et aux nouvelles techniques permises par les progrès numériques.

Essentiellement, pour les données de santé, il est ainsi possible d'identifier la loi informatique et liberté (LIL), précisée par la suite par la directive 95/46 du Parlement européen et du Conseil du 24 Octobre 1995 relative à la protection des personnes physiques à l'égard du traitement de données à caractère personnel et à la libre circulation de ces données[59], transposée en droit interne par la loi du 6 août 2004[60], le Règlement Général relatif à la Protection des Données (RGPD)[61] de 2016, la loi dite « Pour une République numérique » de 2016[62], transposé par la loi du 20 juin 2018 relative

[58] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés

[59] Directive 96/46/CE, Parlement et Conseil, 24 octobre 1995, 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, JOCE L281, 23 novembre, p.31.

[60] Loi n°2004-801, 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, JO du 7 août, n°2.

[61] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016

[62] Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique

à la protection des données personnelles[63], ainsi que les dispositions du Code de la Santé Publique (CSP) et du Code civil.

Bien que les nouveaux textes aient œuvré pour une facilitation de la recherche (terme englobant le développement et la démonstration de technologies, la recherche fondamentale et appliquée, ainsi que la recherche financée par le secteur privé, la loi informatique et liberté, telle que modifiée à la suite de l'entrée en vigueur du RGPD, prévoit un principe d'interdiction du traitement des données de santé, principe connaissant toutefois des exceptions[64].

Le Code de la santé publique, quant à lui, encadre le secret médical[65], l'hébergement des données de santé[66], leur mise à disposition[67], la conformité des systèmes d'information[68], le partage des données[69], l'interdiction de procéder à une cession ou à une exploitation commerciale des données de santé[70].

Cette protection juridique permet de rendre effective la protection souhaitée par l'éthique, à travers le renforcement des droits de la personne concernée et le renforcement des obligations des responsables de traitement.

---

[63] Loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles.

[64] Article 6.1 de la LIL et Article 9.1 du RGPD

[65] Article L1110-4 CSP

[66] Article L1111-8 CSP ; Article R1111-8-8 et suiv. CSP

[67] Article L1460-1 et suiv. CSP

[68] Article L1110-4-1 CSP

[69] Articles R1110-1 et R1110-3 CSP

[70] Articles L1111-8 et L4113-7 CSP

Section 1 : Les droits de la personne concernée par les données de santé

Les données de santé, « données à caractère personnel relatives à la santé physique ou mentale d'une personne physique, y compris la prestation de soins de santé, qui révèlent des informations sur l'état de santé de cette personne »[71], sont extrêmement sensibles et font donc l'objet d'une interdiction de traitement de principe[72], et d'un régime de protection renforcée.

Toutefois, des exceptions sont prévues à ce principe. Ainsi, l'exploitation des données de santé est rendue possible à la condition que la personne concernée, après information, ait consenti de façon claire et explicite[73] au traitement. Il est également possible de procéder au traitement de données de santé 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, ou lorsque le traitement est mis en œuvre par un membre d'une profession de santé, ou par une autre personne soumise à l'obligation de secret professionnel et agissant afin de réaliser des recherches à usage exclusif. Enfin, le traitement de données de santé est permis s'il a pour objet la sauvegarde de la vie humaine (hospitalisation en urgence par exemple, alors le consentement est impossible à obtenir)[74], s'il est conforme aux dispositions de la loi Informatique et libertés et justifié par l'intérêt public, pour éviter notamment la propagation des maladies, ou dans le cadre d'une recherche publique, ou encore s'il s'agit de données anonymisées.

---

[71] Article 4 RGPD

[72] Article 9 RGPD, Article 8 LIL : principe d'interdiction du traitement des données de santé relatives à une personne identifiée ou identifiable et principe d'interdiction de leur commercialisation.

[73] Article 7 RGPD

[74] Article 8, 2° LIL

La première de ces exceptions repose donc sur le principe du consentement éclairé de la personne concernée.

En effet, la loi du 7 octobre 2016 a instauré un droit à l'autodétermination informationnelle, c'est-à-dire un droit à disposer librement de ses données. En parallèle, le RGPD venait renforcer les droits de la personne concernées en 2016 (bien qu'entrant en vigueur en 2018). En conséquence, la loi informatique a été modifiée, et son article premier affirme aujourd'hui que « Toute personne dispose du droit de décider et de contrôler les usages qui sont faits des données à caractère personnel la concernant, dans les conditions fixées par la présente loi ». De ce droit en ont découlé d'autres, au bénéfice des citoyens, qui disposent ainsi de nouveaux outils juridiques, de nouveaux droits afin de mieux contrôler la gestion de leurs données[75].

Néanmoins, les principes essentiels restent les mêmes[76]. Le droit à l'information a ainsi été enrichi de la notion de consentement préalable de la personne concernée au traitement, et le droit d'opposition, le droit à la portabilité des données, le droit à la limitation du traitement ont été ajoutés aux droits de la personnes préexistants.

Le droit positif[77] prévoit ainsi que tout individu dispose du droit d'être informé avant toute communication de ses données à des tiers, et/ou de toute utilisation qu'un tiers en ferait, et de s'y opposer. Au surplus, tout individu peut connaitre l'identité du responsable de traitement et de son DPO, la finalité poursuivie par le traitement auquel les données sont destinées ainsi que le

---

[75] De BRAUX A., LAVOREL L., « GDPR : les enjeux du nouveau règlement européen sur les données personnelles », Revue Fiduciaire, 10 mai 2017.

[76] BRAIBANT Guy, « Droit d'accès et droit à l'information », Mélanges Robert-Edouard Charlier, Ed. de l'Université, 1981.

[77] CLUZEL-METAYER Lucie, DEBAETS Emilie, « Le droit de la protection des données personnelles : la loi du 20 juin 2018 », *RFDA* 2018, p. 1101.

fondement juridique de ce traitement, la durée de conservation des données, les destinataires des données et transferts envisagés hors Union Européenne. Surtout, la personne concernée a le droit d'être informée de l'existence de ses droits d'accès, de rectification ou d'effacement, de limitation et d'opposition, à la portabilité des données, ainsi que de son droit d'introduire une réclamation auprès de l'autorité compétente au niveau national (la Commission Nationale Informatique et Liberté – CNIL – en France).

L'information qui lui est délivrée doit au surplus être transparente, compréhensible et accessible.

La personne concernée dispose ainsi notamment du droit d'accéder aux données la concernant[78], et la notion est entendue au sens large. Elle ne bénéficie toutefois pas aux ayant-droits[79]. Elle dispose de suite du droit de les rectifier, lorsqu'elles s'avèrent inexactes, incomplètes, périmées, ou lorsque leur collecte, utilisation, communication ou conservation était interdite[80].

Elle peut également s'opposer à une mesure de profilage, ainsi qu'au traitement de ses données, pour des « raisons légitimes »[81], jusqu'en 2018, puis pour tout motif depuis l'entrée en vigueur du RGPD[82], sans pouvoir pour autant s'opposer à un traitement rendu obligatoire par la loi, ni à un traitement à des fins de recherche scientifique ou historique ou à des fins statistiques si ce traitement est « nécessaire à l'exécution d'une mission d'intérêt public. Cette dernière impossibilité intéresse particulièrement les hôpitaux publics, qui ont parfois à traiter des données de santé à caractère personnel dans le cadre de recherche scientifique d'intérêt public.

---

[78] Article 39-I-4° LIL

[79] CNIL, « Mort numérique ou éternité virtuelle : que deviennent vos données après la mort ? », 31 octobre 2014.

[80] Article 40 LIL.

[81] Article 38 LIL.

[82] Article 21 RGPD

De même, si la personne concernée dispose d'un droit à l'effacement[83], entendu de manière large et imposant au responsable de traitement de prendre « toutes les mesures raisonnables, y compris les mesures techniques, en ce qui concerne les données publiées sous sa responsabilité, en vue d'informer les tiers qui traitent lesdites données qu'une personne concernée leur demande d'effacer tous liens vers ces données à caractère personnel, ou tout copie ou reproduction de celles-ci »[84], ce droit à l'oubli ne s'applique pas lorsque le traitement s'avère nécessaire à l'exercice de la liberté d'expression, au respect d'une obligation légale, pour des motifs d'intérêt public dans le domaine de la santé publique, à des fins archivistiques, de recherche scientifique ou historique, statistiques ou encore à la constatation, à l'exercice ou à la défense de droits en justice.

Les droits de la personne peuvent s'exercer auprès de la CNIL ou directement auprès du responsable de traitement, auquel incombe, sinon l'obligation de les respecter, d'autres obligations majeures.

[83] Article 17 RGPD

[84] Article 17.2 RGPD

Section 2 : Les obligations à la charge des responsables de traitement de données de santé

Bien que les formalités à la charge des responsables de traitement aient été réduites par le RGPD, elles ont été en partie compensées par la responsabilisation et l'autorégulation à la charge des responsables de traitement. D'une certaine manière, le RGPD a ainsi opéré une révolution en passant d'une logique de discipline externe (procédures d'autorisation, surveillance accrue…) à une logique de discipline interne ; de contrôle interne de la conformité réglementaire. La sécurisation doit ainsi être juridique, technique et organisationnelle. Ce principe est mieux connu sous le nom de principe d'*accountability*.

Dans le cas des données de santé, en raison de l'impact sur les droits et libertés fondamentaux des individus ainsi que de la portée générale et absolue du secret médical, le responsable de traitement doit réaliser une analyse d'impact préalable portant sur les risques techniques de sécurité et les risques juridiques pour la vie privée des personnes concernées.

L'analyse d'impact doit présenter les opérations de traitement et la finalité poursuivie, une évaluation de l'intérêt au regard des risques et les mesures de protection mises en place pour limiter ces risques – anonymisation, certificat SSL, cryptage des données…

Enfin, le droit exige du responsable de traitement qu'il signale à la CNIL, autorité de régulation française, les incidents de sécurité impliquant des données personnelles[85], obligation qui s'ajoute à celle du signalement des incidents informatiques graves aux agences régionales de santé (ARS). D'autre part, des obligations spécifiques sont prévues pour les sous-traitants des opérateurs, lorsqu'ils traitent des données de santé externalisées par un établissement de santé.

[85] Article L1111-8-2 CSP

Ainsi, le formalisme préalable à la mise en œuvre d'un traitement de données a été allégé. Dans le cas des données de santé, appliquées à la recherche, la CNIL a par exemple adopté cinq méthodologies de référence (MR, notamment dans notre cas les MR001, MR003 et MR004), adaptées au cadre juridique en matière de données de santé, et un référentiel pour accéder à certaines données du SNIIRAM[86]. Une demande d'autorisation n'est donc plus nécessaire en cas de déclaration de conformité à l'un de ces méthodologies de référence.

A ce dispositif vient s'ajouter celui des comités de protection des personnes (CPP)[87], prévu à l'article 76 de la LIL. Ces CPP sont notamment sollicités pour les projets impliquant la réutilisation de données de santé et sur la nécessité de recontacter le titulaire des données[88], et évaluent les conditions de validité de la recherche au regard des critères fixés à l'article L1123-5 CSP.

D'autre part, en contrepartie de l'allégement des formalités, les responsables de traitement doivent supporter des responsabilités plus importantes, notamment concernant le respect des droits des personnes concernées.

Au nom de l'obligation de loyauté, le responsable de traitement doit s'assurer que les traitements des données, de manière générale, soient licites, loyaux, adéquats et non-excessifs. Ainsi, l'article 6 du RGPD dispose que :

---

[86] DEMOTES-MAINARD Jacques, CORNU Catherine, GUERIN Aurélie, et alli. « Quel impact du nouveau règlement européen sur la protection des données sur la recherche clinique et recommandations », *Thérapies*, Vol 74 - N° 1 - février 2019, pp. 17-29. Numéro dédié aux XXXIVès Rencontres Nationales de Pharmacologie et Recherche Clinique, pour l'Innovation Thérapeutique et l'Évaluation des Technologies de Santé - Tables rondes Giens – 7 au 8 octobre 2018, organisées par la Société française de pharmacologie et de thérapeutique

[87] Idem

[88] Voir articles L1121-1 à L1126-11 CSP

« Le traitement n'est licite que si, et dans la mesure où, au moins une des conditions suivantes est remplie: a) la personne concernée a consenti au traitement de ses données à caractère personnel pour une ou plusieurs finalités spécifiques ; b) le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci ; c) le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis ; d) le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique ; e) le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement ; f) le traitement est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel, notamment lorsque la personne concernée est un enfant. »

Les données doivent au surplus être exactes et, le cas échéant, mises à jour. Au nom du principe de minimisation, elles doivent également être « adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées »[89].

Pour le cas des données de santé, le principe d'interdiction demeure[90], le consentement de la personne ne suffisant pas à autoriser le traitement, pour les traitements ayant pour finalité la prospection ou la promotion commerciale (même avec des données anonymisées, dès lors que le

[89] DEMOTES-MAINARD Jacques, CORNU Catherine, GUERIN Aurélie, et alli. « Quel impact du nouveau règlement européen sur la protection des données sur la recherche clinique et recommandations », *Thérapies*, Vol 74 - N° 1 - février 2019, pp. 17-29. Numéro dédié aux XXXIVès Rencontres Nationales de Pharmacologie et Recherche Clinique, pour l'Innovation Thérapeutique et l'Évaluation des Technologies de Santé - Tables rondes Giens – 7 au 8 octobre 2018, organisées par la Société française de pharmacologie et de thérapeutique.

[90] LESAULNIER Frédérique, « Recherche en santé et protection des données personnelles à l'heure du Règlement général relatif à la protection des données », *Médecine & Droit*, 2018

professionnel prescripteur est identifiable)[91], ainsi que pour les traitements de données génétiques ayant pour finalité de refuser une assurance à un individu (pour les risques invalidité et décès)[92].

Le responsable de traitement doit en outre garantir la sécurité des données à travers des mesures techniques de protection appropriées (le vocable habituellement employé est celui de *privacy by design* et *privacy by default*). Enfin, les finalités du traitement doivent être déterminées, explicites et légitimes.

Il doit, au surplus, désigner un délégué à la protection des données (DPO, pour Data Protection Officer) et tenir un registre des activités de traitement. Le cas échéant, ils doivent également notifier toute faille de sécurité à la Commission Informatique et Libertés (CNIL) dans les meilleurs délais.

Toutefois, les textes récents, au regard des risques pour la sécurité des systèmes d'information (cyberattaques, failles de sécurité entrainant des fuites…), ont également renforcé le devoir des responsables de traitement de garantir une sécurité suffisante de ces systèmes d'information, contenant les bases de données.

Ainsi, il s'agit désormais d'étudier la protection des données de santé considérées de manière collective, en tant que bases de données.

---

[91] Article L4113-7 CSP

[92] Article L1141-1 CSP

Titre 2 : La protection collective des données de santé : la protection des bases de données

La protection de la vie privée des personnes concernées par des données de santé, considérées cette fois sous leur aspect collectif (« les données de santé », le *big data* en santé ») indispensable afin d'assurer leur consentement au traitement de leurs données, fondé sur la confiance, requiert des « mesures techniques et organisationnelles » appropriées pour garantir que les exigences de la société soient respectées, que les principes de protection des données soient respectés, par défaut et dès la conception des traitements (*privacy by design* et *privacy by default*)

Les données massives, constituées de données personnelles considérées collectivement et à la différence de ces dernières, ne bénéficie pas d'un encadrement juridique très précis ni parfaitement clair. Cependant, du fait de leur attractivité pour des motivations diverses (recherche et innovation médicale, aspect financier…) et du fait de leur caractère particulièrement sensible, ces données massives connaissent actuellement et depuis peu un réel engouement juridique. En effet, face aux risques en termes d'accessibilité et d'exploitation, un droit propre aux données massives s'élabore, fruit de réflexions éthiques, juridiques, économiques et techniques. Ce nouveau domaine juridique, encore parfois embryonnaire, se veut transversal, et touche à la fois le droit de la propriété intellectuelle, le droit public, le droit de la concurrence ou encore le droit de la santé, pour ce qui est des données de santé.

Cependant, les nouvelles règles posées se veulent souvent pragmatiques et, en conséquence, prévoient leurs propres limites, dans une société en mutation, au cœur de laquelle les données prennent une importance majeure, qui ne saurait souffrir d'une insuffisante valorisation.

Chapitre 1 : Une protection réelle

Section 1 : La protection technique des bases de données de santé

Du fait de leur caractère sensible, les données de santé doivent faire l'objet d'une mise en sécurité particulière, afin de garantir leur confidentialité et leur intégrité. La loi informatique et liberté de 1978 a ainsi fait de cette obligation un principe général, dont le non-respect est sanctionné pénalement[93].

Ainsi, concernant les données médicales contenues au sein des dossiers médicaux, par exemple, le Code de Déontologie Médicale[94] prévoit que leur conservation est assumée par les médecins qui en assurent le suivi et qui, incidemment, sont rendus responsables de leur sécurité.

Une délibération de la CNIL en date du 4 février 1997[95] a apporté quelques précisions sur le degré de sécurisation attendu d'un tel traitement. Ainsi, selon cette délibération, le responsable du traitement de données de santé à caractère personnel doit s'assurer de l'effectivité de l'anonymisation de celles-ci et disposer de moyens techniques permettant de la vérifier ; il doit également garantir la confidentialité des données, en recourant au chiffrement de ces données si une telle mesure apparait nécessaire au regard de la sensibilité des données traitées ; il doit de plus prendre des mesures de sécurité appropriées contre les risques de divulgation et d'utilisation détournée des données, notamment grâce au chiffrement ou en restreignant l'accès aux données.

---

[93] Article 226-17 du Code pénal.

[94] Décret n°95-1000, 6 septembre 1995, portant Code de déontologie médicale, JO du 8 septembre, p. 13305.

[95]CNIL, Délibération n°97)008, 4 février 1997, portant adoption d'une recommandation sur le traitement des données de santé à caractère personnel, JO du 12 Avril, p. 5606.

En conséquence, par « mesures techniques et organisationnelles » attendues afin d'assurer une sécurité satisfaisante des données de santé, on peut imaginer[96] :

- Pour les mesures techniques[97] : un chiffrement des données, le recours à des technologies respectueuses de la confidentialité des données (comme le calcul décentralisé), une gestion des droits d'accès, doublée si possible de mots de passe complexes et modifiés régulièrement, la mise en place d'un pare-feu ou d'un antivirus afin d'éviter les malveillances extérieures, l'utilisation de flux sécurisés…
- Pour les mesures organisationnelles : une analyse des risques, la tenue du registre des activités de traitement, la réalisation d'un audit juridique portant notamment sur les contrats (sous-traitance, contrats de travail, contrats de partenariat…), la formation des personnels intervenants sur les données ou à proximité de ces données, etc.

Enfin[98], selon les dispositions de l'article L1110-4-1 du Code de la santé publique, « afin de garantir l'échange, le partage, la sécurité et la confidentialité des données de santé à caractère personnel, doivent être conformes aux référentiels d'interopérabilité et de sécurité élaborés par [ASIP Santé], pour le traitement de ces données, leur conservation sur support informatique et leur transmission par voie électronique : 1° Les systèmes d'information ou les services ou outils numériques destinés à être utilisés par les professionnels de santé et les personnes exerçant sous leur autorité, les établissements et services de santé, le service de santé des armées et tout organisme participant à la prévention ou aux soins dont les conditions d'exercice ou les activités sont régies par le présent code ».

---

[96] CNIL, Guide de la sécurité des données personnelles, consulté en ligne le 20 mai 2019 : https://www.cnil.fr/fr/principes-cles/guide-de-la-securite-des-donnees-personnelles

[97] FIESCHI, M., DUFOUR, J.-C. « *Traitement des données en santé : approches* systémiques », ISTE éditions. (Collection santé, technologies et société: Série Industrialisation de la santé 9), 2018.

[98] CARTAU, C., LOUDENOT, P. « *La sécurité du système d'information des établissements de santé* », Presses de l'École des hautes études en santé publique, 2018.

Section 2 : La protection juridique des bases de données

Avant de pouvoir faire l'objet d'une valorisation – les enjeux économiques notamment étant importants – la base de données de santé nécessite d'être protégée par des dispositifs juridiques[99]. Ceux-ci, du fait de la nature originale de la base de données, sont multiples, encore imparfaits et imprécis[100].

De plus, les bases de données doivent respecter la réglementation sur les données personnelles et l'ordre public. Ainsi, la directive communautaire du 11 mars 1996 sur la protection des bases de données[101], transposée par la loi du 1er juillet 1998[102], a mis en place une double protection pour les bases de données : une protection par le droit d'auteur et une protection par un droit sui generis, c'est-à-dire un droit spécifique au producteur de données. Il est également possible de protéger la base de données par un contrat[103].

La notion de base de données est entrée au sein du Code de la Propriété Intellectuelle (CPI) depuis cette dernière loi, et est définie comme étant un « recueil d'œuvres, de données, ou d'autres éléments indépendants, disposés de manière systématique ou méthodique et individuellement accessibles par des moyens électroniques ou par tout autre moyen »[104].

---

[99] ZOLYNSKI Célia, « Un nouveau droit de propriété intellectuelle pour valoriser les données : le miroir aux alouettes ? », *Dalloz IP/IT* 2018, p.94

[100] BOIZARD Maryline, « La valorisation des données numériques par la protection juridique des algorithmes », *Dalloz IP/IT*, 2018, n°02/2018, p.99

[101] Directive 96/9/CE du Parlement européen et du Conseil, du 11 mars 1996, concernant la protection juridique des bases de données

[102] LOI n° 98-536 du 1er juillet 1998 portant transposition dans le code de la propriété intellectuelle de la directive 96/9/CE du Parlement européen et du Conseil, du 11 mars 1996, concernant la protection juridique des bases de données

[103] MATTATIA F., « Droit d'auteur et propriété intellectuelle dans le numérique », Eyrolles, 2017.

[104] Article L112-3 CPI

La protection des bases de données porte aussi bien sur le contenu que sur le contenant, et peut relever de deux régimes de protection juridique distincts (l'un, l'autre, ou les deux) : la protection par le droit d'auteur et la protection par le droit *sui generis* du producteur de base de données, droit tout à fait particulier.

Le droit d'auteur[105] permet, lorsque la base de données respecter les conditions de protection, notamment la condition de l'originalité (de la forme de la base de données, et non pas de son contenu), de bénéficier du droit moral d'auteur.

Le droit sui generis du producteur de la base de données est, quant à lui, plus complexe. Selon l'article L341-1 du CPI,

« Le producteur d'une base de données, entendu comme la personne qui prend l'initiative et le risque des investissements correspondants, bénéficie d'une protection du contenu de la base lorsque la constitution, la vérification ou la présentation de celui-ci atteste d'un investissement financier, matériel ou humain substantiel.

Cette protection est indépendante et s'exerce sans préjudice de celles résultant du droit d'auteur ou d'un autre droit sur la base de données ou un de ses éléments constitutifs. »

La notion d'investissement substantiel a été ensuite précisée, notamment à travers un arrêt de la Cour de Justice de l'Union Européenne en 2004, et par une décision de la Cour de cassation de 2013.

Ainsi, selon la CJUE, la notion d'investissement « doit s'entendre comme désignant les moyens consacrés à la recherche d'éléments existants et à leur rassemblement dans ladite base. Elle ne comprend pas les moyens mis en œuvre pour la création des éléments constitutifs du contenu

[105] Article L112-3 CPI

d'une base de données ». Pour la Cour de cassation, le caractère substantiel est caractérisé par « les dépenses relatives à la constitution des bases de données »[106], et « plus spécialement, sur les investissements consentis pour la réunion des données pertinentes, leur mise à jour et leur traitement afin de les organiser au sein desdites bases »[107].

Lorsque le droit d'auteur protège la forme, le droit sui generis protège, lui, le contenu de la base de données. Alors que pour le droit d'auteur la condition requise était l'originalité, pour le droit du producteur de la base de données la condition requise pour bénéficier de la protection est un investissement substantiel dans la constitution, la vérification ou la présentation du contenu de cette base. Le producteur de bases de données a alors le droit d'interdire :

« 1° L'extraction, par transfert permanent ou temporaire de la totalité ou d'une partie qualitativement ou quantitativement substantielle du contenu d'une base de données sur un autre support, par tout moyen et sous toute forme que ce soit ;

2° La réutilisation, par la mise à la disposition du public de la totalité ou d'une partie qualitativement ou quantitativement substantielle du contenu de la base, quelle qu'en soit la forme.

Ces droits peuvent être transmis ou cédés ou faire l'objet d'une licence.

Le prêt public n'est pas un acte d'extraction ou de réutilisation. »[108]

---

[106] CJUE, 9 novembre 2004, affaire C-444/02.

[107] Cass. Civ. 1ère ch. 19 juin 2013.

[108] Article 342-2 CPI

Il peut également recourir à des mesures techniques « propres à empêcher ou à limiter les utilisations »[109] de la base.

Toutefois[110], si le producteur de la base de données est une administration ou une personne de droit public, ces droits « ne peuvent faire obstacle à la réutilisation du contenu des bases de données que ces administrations publient »[111], au nom de la politique d'open data.

Si le producteur de la base de données s'avère être un fonctionnaire l'ayant créée « dans l'exercice de ses fonctions ou d'après les instructions reçues », pour des raisons de fonctionnement du service public, son droit moral sur sa création sera réduit[112]. Pour autant, il pourra faire valoir certains droits patrimoniaux : « Dans la mesure strictement nécessaire à l'accomplissement d'une mission de service public, le droit d'exploitation d'une œuvre créée par un agent de l'État dans l'exercice de ses fonctions ou d'après les instructions reçues est, dès la création, cédé de plein droit à l'État.

Pour l'exploitation commerciale de l'œuvre mentionnée au premier alinéa, l'État ne dispose envers l'agent auteur que d'un droit de préférence. Cette disposition n'est pas applicable dans le cas d'activités de recherche scientifique d'un établissement public à caractère scientifique et technologique ou d'un établissement public à caractère scientifique, culturel et professionnel, lorsque ces activités font l'objet d'un contrat avec une personne morale de droit privé. »[113]

---

[109] Article L342-3-1 CPI

[110] DAUTIEU Thomas, GABRIE Emile, « Analyse de l'apport de la loi pour une République numérique à la protection des données à caractère personnel (1ère partie) – L'ouverture de l'accès aux données publiques et sa conciliation avec la protection des données à caractère personnel », *Communication Commerce Electronique*, 2016, n°12, étude 22

[111] Article L321-3 CRPA

[112] Article L121-7-1 CPI

[113] Article L131-3-1 CPI

Cependant, la possibilité pour le fonctionnaire de faire valoir ses droits patrimoniaux est, dans les faits, relativement réduite. En effet, le décret nécessaire à l'application des dispositions susmentionnées n'est pas paru à ce jour, et la mise en œuvre de ce droit dépend pour beaucoup de la politique interne à chaque administration.

Le droit du producteur de la base de données naît à l'achèvement de celle-ci et expire quinze ans après le 1er janvier de l'année civile qui suit celle de son achèvement (article L. 342-5 du Code de la propriété intellectuelle).

Enfin, le créateur d'une base de données peut envisager d'établir des limitations contractuelles à l'utilisation de celle-ci par des tiers (interdiction ou limitation de l'extraction de données par un tiers pour un usage commercial…).

Les dispositifs de protection des bases de données sont cependant limités et ne permettent pas une liberté totale, similaire à celle dont bénéficient les titulaires de droits sur des biens plus consensuels.

Chapitre 2 : Une protection légitimement limitée

Section 1 : Une limitation liée à la non-patrimonialité des données de santé

La protection des bases de données de santé est en partie limitée par la nature numérique de ces données. Cette nature permet en effet de reproduire, partager à l'infini ces données, sans pour autant qu'une dépossession du titulaire des données ait lieu. La question de la patrimonialité des données personnelles fait ainsi l'objet de débats juridiques : les données de santé peuvent-elles circuler et se monnayer comme des biens ordinaires ? Deux courants s'opposent notamment :

- Un premier courant, personnaliste, fait des données personnelles un prolongement de la personnalité des individus ;
- Un second courant, réaliste, patrimonial, considère les données personnelles comme des biens pouvant entrer dans le patrimoine d'un individu et pouvant ainsi fait l'objet d'une non seulement d'une reproduction, mais également d'une cession.

Ainsi, sur le plan juridique, les données de santé « se situent à la frontière entre la personne et la chose, et peuvent relever aussi bien de l'une que de l'autre »[114]. Cependant, en France, la doctrine, la jurisprudence ainsi que le droit positif ont préféré la conception extrapatrimoniale des données. Cette préférence s'observe notamment au sein de la loi du 7 Octobre 2016 pour une République numérique, qui retient un « droit à l'autodétermination informationnelle », tout comme le Conseil d'État, qui considère que, « s'il convient de renforcer la dimension de l'individu acteur dans le droit à la protection des données, c'est en envisageant celui-ci comme un droit à l'autodétermination

[114] MOURON Philippe, « Pour ou contre la patrimonialité des données personnelles », La Revue des médias et du numérique, n°46-47, p. 91, 2018.

plutôt que comme un droit de propriété »[115]. Certains auteurs[116] affirment pourtant que « les textes ne vont pas assez loin dans l'adoption de l'approche personnaliste », et s'opposent fortement à la qualification juridique des données personnelles comme des biens.

En effet, l'approche réaliste aurait pour conséquence de minimiser la composante identitaire et personnelle des données, ainsi que les risques de malveillance et de manipulation des comportements que les traitements peuvent engendrer (discrimination, sélection…). Il s'agit donc de protéger la personne, et non uniquement une valeur, un bien économique. Seule la conception personnaliste peut alors, selon ces auteurs, permettre de garantir une protection réelle de la personnalité des titulaires des données, notamment pour le cas des données de santé, particulièrement sensibles.

Le CCNE, dans son avis n°130, mentionne quant à lui le risque de l'avènement d'une « société de surveillance et de contrôle des individus, par de multiples opérateurs publics ou privés, agissant aux fins les plus diverses, qu'elles soient commerciales, politiques ou sécuritaires », dans le cas où une appropriation sans limite des données était rendue possible.

Juridiquement, il serait ainsi possible de comparer le régime juridique applicable aux données de santé au régime juridique applicable au corps humain et à ses éléments. Les deux sont protégés par le principe d'indisponibilité du corps humain du code civil. Pour les données de santé, le régime de l'« accessoire » suit celui du « principal » : un organe, un cœur, n'est pas appropriable, il en va donc de même de son émanation – un tracé d'électrocardiogramme. Les principes d'indisponibilité et de non-patrimonialité[117] ont été posés par le droit positif afin de garantir le respect du principe de

---

115 Conseil d'État (2014), « Le numérique et les droits fondamentaux », Etudes et documents, n°65, p. 264, La documentation Française.

116 Voir ROCHFELD Judith, « Contre l'hypothèse de la qualification des données personnelles comme des biens », in Les biens numériques, éditions CEPRISCA, pp. 221-236, 2015.

117 Article 16-5 du Code civil.

« dignité » humaine, et ont été discutés lors de plusieurs occasions, notamment lorsqu'il a été techniquement possible de récupérer des éléments et produits du corps humain pour les exploiter et pour qu'ils alimentent un circuit de valeur, sans qu'une atteinte au corps soit nécessaire. Ainsi, par exemple, le sang a pu faire l'objet d'un changement de régime avec une certaine forme de dilution de son lien avec la personne, ce qui a permis de faciliter sa circulation et, incidemment, le développement de médicaments brevetés composés de produits sanguins issus de sa transformation (qui peuvent, aujourd'hui, être cédés à titre onéreux entre professionnels).

Ainsi, le patient, l'usager du système de santé n'est pas propriétaire de ses données de santé, et les institutions recueillant ces données de santé ne peuvent faire valoir de droits de propriété sur ces données, et donc, a fortiori, les revendre.

Dans le cas des données de santé, la frontière entre les données personnelles et les données publiques apparait alors[118]. Une circulaire du 14 février 1994[119] distinguait ainsi les données selon qu'elles étaient publiques (données brutes, élémentaires, sans mise en forme originale) ou non (données enrichies, à valeur ajoutée), ces dernières étant, elles, susceptibles d'appropriation. Néanmoins, cette distinction tend à devenir de plus en plus difficile à opérer en pratique, la frontière entre les deux étant poreuse, et les administrations détenant des données (données de santé pour le cas des hôpitaux), devant respecter les principes d'accessibilité et de réutilisation dans le cadre de la politique d'open data et d'open governement[120], ne font désormais plus valoir de droits exclusifs sur ces données. Les données semblent revêtir, de plus en plus, la qualité de « biens communs ».

---

[118] CHEVALLIER Jacques, CLUZEL-METAYER Lucie, « Introduction », RFAP, 2018/3, n°167, pp. 463-470.

[119] Circulaire du 14 février 1994 relative à la diffusion des données publiques, JORF n°42 du 19 février 1994 page 2864.

[120] BOUL Maxime, « Réflexions sur la notion de donnée publique », RFAP, 2018/3, n°167, pp. 471-478.

Section 2 : Une non-patrimonialité des données de santé critiquée

Bien que la France ait préféré la conception personnaliste, extrapatrimoniale des données, des voix s'élèvent de nombreux horizons afin de faire reconnaitre un droit de propriété sur les données personnelles. Les défenseurs de cette conception arguent notamment de la valeur économique des données[121], ainsi que l'absence théorique d'inconvénients de l'utilisation des données par un tiers pour le titulaire des données.

Le fait est qu'actuellement, la valorisation des données a souvent lieu de manière occulte (cookies récupérés sur les sites internet, données récupérées à la suite de l'acception de conditions d'utilisation par un utilisateur qui n'en a pourtant pas pris connaissance…), en échange d'un service « gratuit » : accès à un site internet, à des informations, à un réseau social… De ce manque de transparence en défaveur des utilisateurs et producteurs de données sont ainsi nées des revendications portant sur une réappropriation des données par leurs titulaires, afin qu'ils puissent également se réapproprier leur valeur – économique notamment – et qu'ils puissent assurer plus efficacement la confidentialité de leurs données sensibles par une surveillance plus efficace.

Cette volonté s'appuie également sur l'apparition de nouvelles technologies, la blockchain notamment, qui permettrait aux citoyens de contrôler leurs données de leur collecte à leur utilisation.

En effet, à ce jour, les données de santé ne sont protégées, grâce au RGPD et à la loi informatique et libertés notamment, qu'à travers la conception personnaliste des données, qui entend protéger la vie privée des titulaires de données, et par les droits que cette conception a créée au bénéfice de ceux-ci. Ces textes reposent sur l'autorégulation et sur une responsabilisation des acteurs, et les

---

[121] Le Monde, « Inventer un droit patrimonial sur les données de santé », 12 janvier 2019, p.7.

Génération Libre, « Rapport Mes datas sont à moi – Pour une patrimonialité des données personnelles », Janvier 2018.

droits qu'ils créent au bénéfice des personnes concernées, s'ils ne sont pas respectés, peuvent amener le responsable de traitement à subir une sanction ou l'obliger à réparer le dommage subi.

Cette logique permet donc aux citoyens d'agir *a posteriori*, mais les citoyens ne disposent pas d'outil leur permettant de contrôler l'usage qui est fait de leurs données *a priori*. La *blockchain*, en tant que technologie de stockage et de transmission d'informations, permettrait de fournir un tel outil de contrôle *a priori*. Les données de santé pourraient ainsi être partagées de manière cryptée, et décryptées uniquement après consentement au partage de la personne intéressée.

D'autre part, d'autres technologies sont actuellement développées et sont liées à la technologie *blockchain*, notamment la technique du calcul décentralisé. Ce calcul décentralisé ouvre la possibilité de fournir à un utilisateur final non plus une multiplicité de données personnelles individuelles, mais une cohorte de données agrégées, ce qui permettrait de renforcer la confidentialité des données.

Ainsi, théoriquement, « le citoyen devrait pouvoir autoriser l'exploitation de ses données, sous forme de licences, pour des finalités définies, et être rémunéré en redevances. Cela garantirait le respect des droits des personnes concernées et un juste partage des revenus liés aux échanges. Il faudra alors distinguer entre données « inaliénables » tenant à l'essence de la personne (nom, âge…) et celles qui, dissociables, représentent un actif économique. »[122]

[122] Le Monde, « Inventer un droit patrimonial sur les données de santé », 12 janvier 2019, p.7.

Partie II : La valorisation des données de santé

Du fait de l'augmentation exponentielle de leur nombre et des multiples applications permises par leur exploitation, les données massives en santé font désormais l'objet de nombreuses convoitises, le secteur public comme le secteur public y voyant une matière première source d'innovation. Ainsi, les données massives en santé peuvent être utilisées dans le domaine de la recherche (publique, privée, partenariale), dans la prise en charge des patients et l'organisation du système de soins. Au surplus, les données de santé peuvent être utilisées pour développer des outils de bien-être, ou encore pour appuyer des demandes administratives (autorisation de mise sur le marché, demande de remboursement…), de la part des entreprises du secteur privé. Intérêts public et privé semblent donc tous deux concernés par les données massives en santé et leurs exploitations.

Néanmoins, ces exploitations, du fait des mutations technologiques et culturelles qu'elles impliquent, obligent à mener une réflexion profonde, liée comme nous l'avons vu plus tôt au recueil des données, à leur traitement, mais également liée à leur exploitation, leur utilisation et réutilisation, voire leur cession.

En effet, face à cet engouement, la question de la valorisation des données de santé se pose d'un point de vue triple : éthique, juridique et économique : que valent les données de santé ? S'il est seulement possible de déterminer une valeur pour ces données, peut-on imaginer, éthiquement, juridiquement, la maximiser, notamment par des activités commerciales ?

Le concept de valorisation des données fait référence à la problématique de la production de valeur générée à partir des données collectées par une organisation. Le champ de la valorisation des données est très large : les données peuvent être valorisées à des fins de recherche scientifique (données médicales, sociologiques, etc.), à des fins de sécurité, à des fins d'optimisation de la gestion d'un établissement, à des fins sociétales, etc. La valorisation des données peut se faire en interne

ou en externe (par le partage de données à des tiers, soit avec monétisation de la donnée, soit par un dispositif d'open data qui permet une valorisation sociale).

La valorisation des données de santé peut donc être considérée sous deux aspects. Le premier consiste en une valorisation financière, commerciale et revêt la plupart du temps la forme d'un transfert de technologie (concession d'une licence ou création d'une entreprise dérivée…) ou la commercialisation d'un produit ou d'un service. Le second consiste en une valorisation non-marchande, sociale, par le développement de solutions et d'applications dont l'intérêt dépasse le seul intérêt privé.

Ainsi, deux considérations cohabitent au sein de la notion de valorisation : un intérêt économique d'une part, un intérêt éthique et sociétal d'autre part : la valorisation économique se distingue de la valorisation non-économique.

Ces deux intérêts, passés aux prismes des données de santé et du service public hospitalier, apparaissent tantôt incompatibles, tantôt compatibles, complémentaires, l'un pouvant parfois même devenir indispensable à la survie de l'autre.

En cela, le droit entend opérer une conciliation entre ces intérêts en encadrant les pratiques relatives à la valorisation des données de santé. Le droit, outil politique, est ainsi élaboré en fonction d'une société et de ses attentes, tant en matière économique qu'éthique.

Ainsi, le droit actuel en matière de valorisation des données de santé encadre-t-il une complexe réalité considérée comme nécessaire au regard d'intérêts à la fois éthiques et économiques (Titre 1), malgré un flou certain (Titre 2), illustrant la volonté de permettre la mise en œuvre un processus de valorisation économique du recours aux données de santé à la fois performant, efficient et respectueux du cadre juridique et de principes éthiques.

Titre 1 : La valorisation des données de santé au sein du Service Public Hospitalier : une complexe réalité

La diffusion du numérique dans notre système de santé, effectuée à un rythme rapide, est aujourd'hui largement menée au sein des établissements de santé, notamment les Centre Hospitalier Universitaires (CHU), créés en 1958 par les ordonnances Debré[123]. Ceux-ci sont doublement intéressés par le numérique : d'une part, ils produisent, dans leurs activités de soins, de nombreuses données, et sont amenés, de par leurs fonctions et leur taille, à devenir des centrales de données à l'échelle territoriale ; d'autre part, ils pourraient gagner beaucoup à valoriser ces données, en les mobilisant en interne ou en les mettant à disposition de partenaires extérieurs à des fins d'innovation dans le domaine du soin, de l'enseignement et de la recherche, missions essentielles des CHU, ou encore à des fins d'amélioration de la gestion, de la qualité, etc.

Néanmoins, la mobilisation de ces données, leur traitement et leur organisation afin de garantir leur qualité, implique que de nouvelles compétences soient développées ou introduites au sein des établissements de santé. Ces nouvelles compétences (data management, data science, ingénierie informatique, etc.) sont cependant rares et, donc, coûteuses. Dans un contexte financier contraint[124], la valorisation des données de santé implique donc de rendre l'exploitation de ces

---

[123] Ordonnance n° 58-1198 du 11 décembre 1958 portant réforme de la législation hospitalière.

Ordonnance n°58-1373 du 30 décembre 1958 relative à la création de centres hospitaliers et universitaires, à la réforme de l'enseignement médical et au développement de la recherche médicale. Décret n° 58-1202, portant réforme hospitalière.

[124] « En 2015, pour la troisième année consécutive, les comptes financiers des hôpitaux publics continuent de se dégrader. Leur déficit atteint 400 millions d'euros, soit environ 0,6 % des recettes. » ; « Cette détérioration de la situation financière concerne notamment les centres hospitaliers régionaux hors AP-HP ». Une amélioration est néanmoins à noter en 2016. « L'amélioration de la situation financière concerne notamment les centres hospitaliers régionaux (CHR).
Source : DREES, Panorama des établissements de santé, éditions 2017 et 2018.

données viable financièrement pour les établissements ; il s'agit alors de trouver de nouvelles sources de financement pour ces nouvelles activités.

Ainsi, étudier la question de la valorisation des données de santé implique d'étudier, individuellement et de manière transversale, d'une part la question de la valorisation du patrimoine immatériel des personnes publiques, notamment de leurs bases de données, et d'autre part la question des activités économiques subsidiaires des établissements de santé avec ou sans partenariat industriel.

Au surplus, la valorisation des données de santé connait de nombreuses spécificités liées au statut de la donnée, à leur caractère personnel ainsi qu'à leur caractère stratégique.

Cette matière, appréhendée par le droit, apparait donc particulièrement complexe et subtile.

Bien que la volonté politique affichée soit celle d'une préoccupation croissante pour la question de la valorisation du patrimoine immatériel des personnes publiques, notamment de leurs données de santé, ce domaine apparait toujours en cours de construction et fait l'objet de nombreuses interrogations, notamment de la part des professionnels du droit, du fait de sa complexité.

Il induit en effet le recours à plusieurs sources juridiques, à la fois internationales (plus particulièrement communautaires : traités, règlements, directives européens…) et nationales (comme, par exemple, la loi informatique et liberté de 1978 modifiée, la loi de modernisation de notre système de santé de 2016, les dispositions du code de la santé publique, de la propriété des personnes publiques, de la propriété intellectuelle, des relations entre le public et l'administration, les décrets, ordonnances, circulaires, textes parus ou en attente de parution…).

La valorisation des données de santé pose également des questions éthiques, liées par exemple au bien-fondé de l'utilisation des données de santé, à la protection de la vie privée des personnes concernées, ou encore à la valeur (terme entendu au sens large) conférée à la donnée.

Face à ces interrogations et à un certain flou juridique, il revient souvent aux administrations publiques, aux hôpitaux, de déterminer et de développer elles-mêmes leurs stratégies en matière de valorisation de leur patrimoine de données de santé, de manière plus ou moins autonome : certains établissements peuvent décider de se concerter, à l'échelle nationale, afin de trouver des solutions et des outils communs.

Des réflexions sont ainsi menées actuellement dans ce domaine, à la fois au sein de certains centres hospitaliers, notamment des CHU, souvent amenés à mettre en commun leurs expériences (au sein de groupes de travail au niveau national…) mais également au sein d'administrations centrales, d'agences, de missions commanditées au niveau national (travaux du Health Data Hub, de la DREES…).

Aussi, la valorisation des données de santé, domaine en construction, est aujourd'hui l'objet de nombreuses discussions (Chapitre 1) et le contexte politico-juridico peut parfois sembler complexe, empêchant une valorisation ambitieuse (Chapitre 2).

Chapitre 1 : La valorisation des données, sujet de controverses.

Section 1 : La valeur des données de santé

Aujourd'hui, les Nouvelles Technologies de l'Information et de la Communication (NTIC) jouent un rôle majeur et central, et le domaine de la santé est particulièrement impacté par l'avènement, la multiplication et la montée en puissance de ces nouvelles technologies. La médecine moderne induit ainsi, de plus en plus, l'utilisation de données personnelles numérisées.

Néanmoins, l'exploitation des données personnelles de santé est un sujet sensible, celles-ci ayant trait à l'intimité de chaque individu. Des craintes et des incertitudes peuvent alors naître au sein de la société. Afin d'éviter une « crise de confiance », qui pourrait à terme empêcher l'exploitation des données de santé, et donc leur valorisation, il importe alors de mieux connaître, de mieux comprendre les données de santé et les modalités de leur exploitation, mais également de mieux communiquer autour de l'usage des données de santé, dans l'optique de protéger l'individualité, la vie privée, les droits de chaque citoyen.

Ainsi, face à la volonté de valoriser les données de santé, des questionnements éthiques et moraux sont rapidement venus se confronter aux questionnements économiques et juridiques.

Interroger la donnée personnelle de santé sous l'angle éthique demande tout d'abord de s'intéresser à sa valeur[125]. Il s'agit alors de définir la valeur intrinsèque de la donnée pour ensuite en déduire une valeur informative et d'exploitation.

a. La valeur intrinsèque de la donnée

Il est habituellement considéré que les données n'ont pas de valeur intrinsèque : fixer un prix fixe sur une donnée ou sur un jeu de données semble particulièrement difficile. Cependant, il serait vain d'affirmer que les données n'ont pas de valeur : un marché de la donnée existe. La problématique de la valeur des données est donc le fruit d'un paradoxe : la donnée n'a pas de valeur mais les données en ont[126].

Ainsi, la valeur intrinsèque de la donnée dépend de sa qualité conçue comme l'absence d'altération de la donnée et l'assurance de son exploitabilité (c'est à dire de son format numérique notamment), tout au long du parcours de transmission (obtention, traitement, conservation, diffusion). Cinq éléments peuvent ainsi être identifiés pour caractériser la qualité d'une information médicale : l'intégrité, l'exactitude, la précision, la validité et l'authenticité. L'existence de ces critères dépend de la qualité des Systèmes d'Information Hospitaliers (SIH), de leurs produits et services.

b. La valeur informative de la donnée

La valeur informative de la donnée, découlant directement de la valeur intrinsèque de la donnée, sera quant à elle liée au sens qu'on peut lui donner, et sera intimement dépendante du contenu de la donnée, de la diversité, la qualité et la quantité des données disponibles. Contrairement aux

---

125 BERANGER Jérôme, « La valeur éthique de la donnée de santé à caractère personnel : vers un nouveau paradigme de l'écosystème médical dématérialisé », *Sciences de la société*, 95 / 2016, mis en ligne le 05 Juillet 2016, consulté le 12 Avril 2019.

126 HERVE Christian, STANTON-JEAN Michèle, MARTINENT Eric (dir.), « Les systèmes informatisés complexes en santé – Banque de données, télémédecine : normes et enjeux éthiques », *Dalloz*, Thèmes et commentaires, Actes, 2013

principes économiques traditionnels, il semblerait que la puissance économique, la valeur de la donnée ne réside non-pas dans sa rareté, mais au contraire dans l'importance de ses quantités : leur valeur augmente en fonction de la quantité, mais également, enfin, et de leur traitement ou de la possibilité d'un tel traitement.

c. La valeur d'exploitation de la donnée

En effet, la valeur d'exploitation, d'usage de la donnée sera, elle, liée à la stratégie de partage, de diffusion de la donnée (transmettre la bonne information, au bon moment, à la bonne personne), ainsi qu'à la satisfaction finale de l'usager du système de santé (création, développement, amélioration d'un produit ou d'un service de soin). La portée causale potentielle de ces actes induit une responsabilisation importante des acteurs impliqués, laquelle requiert donc que soient appliqués des principes éthiques forts, tels que ceux de Bienfaisance, d'Autonomie, de Non-malfaisance et de Justice, tels qu'identifiés par Beauchamp et Childress comme étant les principes fondamentaux de l'éthique médicale[127]. L'application de ces principes permettra alors d'équilibrer la relation entre protection et exploitation des données personnelles de santé, laquelle évolue selon les données elles-mêmes, mais également selon les objectifs, les enjeux, le sens, de l'usage qui est en est fait, par qui et comment, *etc.*

Afin d'augmenter la valeur informative et la valeur d'exploitation de la donnée, donc sa valeur d'usage, il peut être envisagé d'opérer une hiérarchisation sélective de ces données[128]. Cette sélection aurait ainsi une action positive sur le principe de bienfaisance (efficience de la communication et donc de la prise en charge médicale), d'autonomie (efficience de l'information –

[127] BEAUCHAMP T.L., CHILDRESS J.F., « Les principes de l'éthique biomédicale », Médecine et Droit, volume 2008, n° 89 (mars-avril 2008), p.59 (traduit de l'américain).

[128] BERANGER Jérôme, « La valeur éthique de la donnée de santé à caractère personnel : vers un nouveau paradigme de l'écosystème médical dématérialisé », Sciences de la société, 95 / 2016.

claire, précise, adaptée et compréhensible – faite au patient, garantissant son consentement éclairé, donc son autonomie), de non-malfaisance (l'accès limité aux données garantissant leur confidentialité et leur protection). En revanche, le principe de Justice serait atteint de manière négative, l'équité l'emportant sur l'égalité, sur le principe d'une discrimination positive. L'on pourrait également craindre que l'intégrité des données soit altérée.

En conséquence, il apparait complexe de trouver un équilibre entre la disponibilité des données de santé, leur confidentialité et leur protection, et il importe donc de faire appel à l'éthique, à la déontologie, à l'humain pour garantir la protection et la confidentialité des données personnelles de santé. Aussi, il peut apparaitre souhaitable de mettre en place une charte éthique en matière de conception, mise en place et usage des données personnelles de santé, favorisant les bonnes pratiques tout en assurant et en facilitant la création, le partage et la diffusion de ces dernières.

Mener une réflexion éthique sur les procédures de contrôle et d'encadrement des données au regard de leur valeur permettrait ainsi de conserver une forte protection des données, et donc une forte confiance de la part des producteurs et fournisseurs de données, ce qui contribuerait à maitriser les risques inhérents à l'exploitation de données.

Section 2 : La valorisation des données et l'éthique

D'autre part, la question de la valeur de la donnée induit une réflexion sur la pertinence et l'éthique du partage de la donnée, mais également sur l'aspect éthique des finalités de la valorisation de ces données.

Les travaux montrant les possibilités induites par l'utilisation des données massives en santé sont légions, et démontrent souvent des aspects bénéfiques de cette valorisation[129]. L'IA en santé notamment serait un « accélérateur de progrès médical » et une « source d'économie prodigieuse »[130].

Ainsi, l'utilisation des données en santé enthousiasme de nombreux acteurs : les chercheurs y voient une source de connaissances nouvelles, le corps médical un moyen de développer ou d'améliorer des thérapeutiques ou des outils diagnostiques. Le corps de direction des établissements de santé y voit un moyen d'améliorer la qualité de la prise en charge, la gestion de l'établissement, les patients un outil de transparence. Les entreprises privées, grandes industries ou « start-up », y voient un bénéfice potentiel par la création de services innovants et par la création de valeur[131]…

Ces promesses amènent en conséquence un engouement important de la part de la plupart des acteurs du secteur sanitaire ou liés à ce secteur. Pour cette raison, la puissance publique, à travers

---

[129] DIEBOLT Vincent, AZANCOT Isaac, BOISSEL François-Henri, et alli, « « Intelligence artificielle » : quels services, quelles applications, quels résultats et quelle valorisation aujourd'hui en recherche clinique ? Quel impact sur la qualité des soins ? Quelles recommandations ? », *Thérapies*, Vol 74 - N° 1 - février 2019, pp. 141-154. Numéro dédié aux XXXIVès Rencontres Nationales de Pharmacologie et Recherche Clinique, pour l'Innovation Thérapeutique et l'Évaluation des Technologies de Santé - Tables rondes Giens – 7 au 8 octobre 2018, organisées par la Société française de pharmacologie et de thérapeutique.

[130] Ibidem

[131] CCNE, Avis 130 sur « Données massives (big data) et santé : une nouvelle approche des enjeux éthiques », paru le 28 mai 2019

un travail de réflexion éthique, social, juridique, technique… se doit d'intervenir afin d'encadrer le développement et la réalisation de ces promesses, tout en conservant une prudence nécessaire face aux risques inhérents à l'innovation. Les pouvoirs publics influent donc sur les modalités de la valorisation des données de santé afin de concilier innovation et éthique en minimisant les risques.

Afin de les rendre éthiquement viables, les modalités de valorisation des données de santé doivent être réfléchies, pensées et réalisées au travers d'une réflexion éthique.

Ainsi, il importe de mener une réflexion éthique sur la démarche de valorisation des données de santé, au sein de laquelle nous pouvons identifier 3 aspects majeurs :

- La nature des données valorisées, c'est-à-dire leur qualité et leur caractère identifiable ;
- La nature responsable du traitement des données ainsi que le lien de confiance qui l'unit avec le titulaire des données ;
- La nature du traitement réalisé afin de valoriser les données : à des fins industrielles, de recherche, de gestion…

Ainsi, selon un sondage Odoxa pour le Healthcare Data Institute[132], « 72% des Français estiment que leurs données de santé sont utiles pour faire avancer la recherche et la santé pour tous, et plus de 8 Français sur 10 (83%) accepteraient de partager leurs données de santé si cela répondait à certains objectifs. Parmi ces objectifs, deux réunissent la majorité des Français : l'amélioration des diagnostics et des traitements médicaux (53%) et la progression plus rapide de la recherche médicale (51%).

[132] Sondage Odoxa pour le Healthcare Data Institute, 16 Novembre 2017 :
http://www.odoxa.fr/wp-content/uploads/2017/11/CP-HDI-Odoxa-16nov17.pdf

Les Français n'accordent en revanche pas une confiance aveugle et attendent que certaines conditions soient remplies[133].

S'ils ne sont que 14% à affirmer qu'ils ne transmettraient leurs données de santé à personne au-delà des personnels de santé qui les traitent, seuls 6% le feraient sans aucune condition. Tous les autres accepteraient de le faire à certaines conditions : au-delà de l'anonymat et de la sécurisation de leurs données, 52% des Français les partageraient à condition de savoir à quelles fins elles seront potentiellement utilisées, 51% de savoir exactement à qui leurs données seront transmises et 50% de pouvoir faire valoir leur droit d'opposition à tout moment. »

La confiance repose donc sur deux impératifs : l'exigence d'une information compréhensible, adaptée et loyale concernant le recueil des données, leur conservation, les mesures de sécurité et de confidentialité et l'intelligibilité de leur traitement et la possibilité de faire valoir ses droits sur ses données.

Au surplus, le sondage révèle qu'une majorité de Français (65%) « fait confiance aux institutions françaises pour mettre en place les conditions nécessaires à la protection de leurs données de santé mais seuls 10% en sont persuadés. Il s'agit donc d'une confiance fragile qui peut être remise en cause par la moindre affaire de piratage », ou par la survenance d'un scandale dans ce domaine.

L'éthique des finalités de la valorisation doit donc être, également, étudiée afin de correspondre aux attentes de la société (qui, majoritairement, souhaite mettre ses données au service de la recherche).

Les données de santé peuvent servir d'une part la recherche, mais également d'autre part le développement de nouveaux algorithmes, nouvelles technologies numériques, informatiques, de

[133] CCNE, Avis 130 sur « Données massives (big data) et santé : une nouvelle approche des enjeux éthiques », paru le 28 mai 2019.

communication (Intelligence Artificielle notamment), il est indispensable d'étudier ces produits finaux d'un point de vue éthique afin de déterminer la valeur éthique de la donnée.

Tout d'abord, l'exploitation des données de santé peut mener à des travaux de recherche en santé (utilisation de l'IA en recherche clinique notamment). Ces travaux peuvent avoir un impact extrêmement positif, par exemple pour le développement des connaissances médicales, l'amélioration des pratiques cliniques ou l'amélioration de la santé publique (par une prévention plus ciblée, par exemple).

Notamment, l'usage des données de santé présenterait[134] un impact positif (« apport potentiel et bénéfice théorique ») sur les pratiques de recherche et les mentalités des chercheurs, grâce aux possibilités d'auto apprentissage par le traitement successif et répétitif de données et par une capacité d'adaptabilité. L'usage des données permettrait de réaliser des innovations médicales dans deux domaines de recherche :

- La recherche clinique (ex : développement de nouvelles molécules, réduction du taux d'échec en matière de médicaments testés…) ;
- La recherche pour l'amélioration de l'efficience et de la coordination des soins (ex : génération de conversation ou de contenu multimédia, gestion des flux, etc…).

D'autre part, l'exploitation des données de santé peut mener à l'élaboration de nouvelles technologies, notamment d'intelligence artificielle, ou de nouvelles applications de « bien-être ».

---

134 DIEBOLT Vincent, AZANCOT Isaac, BOISSEL François-Henri, et alli, « « Intelligence artificielle » : quels services, quelles applications, quels résultats et quelle valorisation aujourd'hui en recherche clinique ? Quel impact sur la qualité des soins ? Quelles recommandations ? », *Thérapies*, Vol 74 - N° 1 - février 2019, pp. 141-154.

Ici, certaines craintes sont exprimées quant à l'utilisation des données massives en santé. Ainsi, une crainte persistante tient en la possible supplantation de l'humain par l'IA.

Cependant, face à cette crainte, de nombreuses voix affirment qu'il n'en sera rien. Au contraire, certains soutiennent que l'IA permettra de redonner de l'importance à l'humanité, en lui permettant de se différencier de l'intelligence purement logique, et en mettant en avant son empathie et ses relations sociales. Au surplus, l'humanité pourrait, grâce à sa différenciation de l'IA, gagner en valeur (un service rendu par un être humain aurait plus de valeur – économique, sociale, etc. – qu'un service rendu par une machine dotée d'une intelligence artificielle)[135].

A l'étape du développement de produits issus de la valorisation des données de santé, notamment des technologies d'IA, le comité notait également une dilution de la responsabilité possible dans le cas du recours à des technologies d'aide au diagnostic, à la prescription, à la décision médicale.

Ainsi, par exemple, afin de ne pas freiner la valorisation des données, un consensus semble avoir été trouvé autour du « principe de garantie humaine », qui veut que, lorsqu'un choix médical doit être fait et qu'il est appuyé par une technologie d'aide à la décision, la décision finale soit une décision humaine. Il importe au surplus que la personne soit informée du recours à un algorithme d'aide à la décision médicale dans son parcours de prise en charge. Le CCNE a ainsi rappelé que « ces technologies doivent rester une aide à la décision humaine, excluant toute automatisation de la décision médicale et que doit être préservée l'écoute du patient, les données ne pouvant remplacer le dialogue ».

---

[135] Guillaume Saupin, « L'IA donnera plus de valeur à la présence humaine », Les Echos, 20 Juin 2019. https://www.lesechos.fr/idees-debats/cercle/lia-donnera-plus-de-valeur-a-la-presence-humaine-1030974#xtor=CS1-26

Néanmoins, la question de la formation des professionnels subsiste. En effet, l'aspect « humain » de la pratique médicale a, dans les dernières années, connu une perte d'importance : développement important de la robotisation médicotechnique, développement des logiciels d'aide à la décision ou à la prescription médicale, développement de la réalité virtuelle en chirurgie… Il s'agira donc, dans les années à venir, d'assurer que les médecins conservent et développent l'humanité de leur art, dans un contexte de multiplication des outils numériques les distanciant potentiellement de leurs patients, et que soit ainsi renforcée la relation humaine entre soignants et soignés.

Enfin, il importe, tout au long du processus de valorisation des données de santé, de gérer le risque d'accroissement des inégalités de santé liée à la diffusion du numérique (fracture numérique), à la fois pour les patients et pour les soignants : tout le monde ne dispose pas des compétences et connaissances utiles afin d'appréhender convenablement les nouvelles technologies numériques.

Chapitre 2 : Valoriser les données de santé, une possibilité complexe à appréhender

Section 1 : La valorisation des données face à la politique d'ouverture des données (open data)

Les administrations sont naturellement amenées à produire, collecter ou stocker des données de par leurs missions et activités. Pour le cas de l'hôpital, ces données sont la plupart du temps des données de santé, liées à la prise en charge des patients – données de diagnostic, de soin, de recherche…

Parmi les biens publics, les données publiques font cependant l'objet de nombreuses discussions juridiques, balançant entre les logiques patrimoniales (valorisation des données) et les logiques d'open data (ouverture des données, impliquant l'accès aux données, le droit de réutilisation, le droit à l'information administrative). Ces discussions se justifient en effet par la confrontation entre une certaine exigence démocratique (protection des données et respect des choix de société) et le potentiel économique immense des données publiques[136].

[136] MARCHAND Jennifer, « L'open data, la réutilisation des données publiques entre exigence démocratique et potentiel économique », *JCP A.*, 17 févr. 2014, n° 7, p. 2038.

Les pouvoirs publics[137] nationaux comme communautaires, ainsi que les juges[138][139], se sont donc saisis de la question, à plusieurs reprises. Le droit positif en la matière reste cependant épars et complexe à visualiser dans sa totalité, rendant en conséquence difficile l'appréciation de la notion de « donnée publique » et la délimitation du concept d'ouverture des données[140]. Certains affirment ainsi qu'il est peu efficace et peu cohérent[141].

Actuellement, la tendance est à l'ouverture des données publiques[142], laquelle est équilibrée par l'existence d'une réglementation sur l'utilisation des données personnelles (cf : Partie 1). Cette ouverture a été amorcée dès 1978 par la loi du 17 juillet 1978[143], puis par une directive européenne

---

[137] Avec, par exemple :
- La 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 ;
- La loi n° 2015-1779 du 28 décembre 2015 relative à la gratuité et aux modalités de la réutilisation des informations du secteur public ;
- La loi n° 2016-1321 du 7 octobre 2016 pour une République numérique.

[138] Avec, par exemple :
- La décision du Conseil Constitutionnel n°2017-752 DC du 8 septembre 2017, Loi pour la confiance dans la vie politique (JO 16 septembre 2017, texte n°5) ;
- L'avis du Conseil d'Etat du 21 novembre 1972, Ofrateme, n°309721 ;
- L'arrêt CE, Ass., 10 juillet 1996, Sté Direct Mail Promotion et a., rec. P.277 ;
- L'arrêt CE, 24 juillet 2006, CEGEDIM, req. N°247769.

[139] Voir également : Conseil d'Etat (2014), « Le numérique et les droits fondamentaux », Etudes et documents, n°65, La documentation Française

[140] CAMUS Aurélien, « La propriété des données publiques », *RFAP*, 2018/3, n°167, pp. 479-490.

[141] Comme l'économiste André LOTH :

https://drees.solidarites-sante.gouv.fr/IMG/pdf/rapport-donnees-de-sante-2013-presentation19-12-2013.pdf

[142] YOLKA Philippe, « Open Data : L'ouverture, c'est l'aventure », AJDA, 2016, p. 76.

[143] 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

dite ISP[144] du 17 novembre 2003, transposée en 2005[145] dans le droit français. Il a ensuite évolué jusqu'à aboutir au texte de la loi du 28 décembre 2015[146] pour le cadre général.

L'objectif de ces différents textes était, entre autres, de promouvoir un mode de gouvernement transparent, plus ouvert et ainsi plus efficace en permettant à chaque citoyen de disposer, gratuitement, des informations dont l'appareil administratif de l'État dispose[147]. Il s'agissait également d'accélérer l'activité économique et la croissance économique[148].

La loi de 1978 prévoit ainsi que l'accès aux documents administratif peut se faire à travers deux moyens : la communication ou la diffusion des documents. En principe, certains types de documents doivent obligatoirement être publiés, et selon l'article 7 de cette loi, les administrations sont autorisées à diffuser l'ensemble des documents librement communicables.

Cependant, les documents ne sont pas toujours communicables[149], et il importe de rester vigilant quant à la nature des informations livrées au public, afin de garantir le respect des secrets et informations protégés. Cette affirmation apparait d'autant plus fondamentale à l'hôpital, qui, en tant qu'administration publique, est soumis au principe d'open data, mais qui, du fait de ses missions spécifiques, doit veiller à la confidentialité des données personnelles et sensibles (de santé) dont il dispose.

---

144 Dir. 2003/98/CE.

145 Ordonnance n° 2005-650 du 6 juin 2005 relative à la liberté d'accès aux documents administratifs et à la réutilisation des informations publiques.

146 Loi n° 2015-1779 du 28 décembre 2015 relative à la gratuité et aux modalités de la réutilisation des informations du secteur public.

147 VERDIER Henri, VERGNOLLE Suzanne, l'État et la politique d'ouverture en France, AJDA 2016, p. 92.

148 TROJETTE Mohamed Adnène, « Ouverture des données publiques. Les exceptions au principe de gratuité sont-elles toutes légitimes ? », rapport au Premier Ministre, juillet 2013

149 VERDIER Henri, VERGNOLLE Suzanne, l'État et la politique d'ouverture en France, AJDA 2016, p. 92..

Dans le domaine des données de santé, c'est ainsi que la loi de modernisation de notre système de santé, promulguée le 26 janvier 2016[150], prévoit l'ouverture des données agrégées de santé à des fins de recherche, d'étude ou d'évaluation d'intérêt public, à tout citoyen, professionnel de santé ou organisme (public ou privé) participant au fonctionnement du système de santé et aux soins.

Cependant, le législateur a entendu fixer des conditions d'ouverture de ces données. Ainsi, les données susceptibles d'être publiées ne doivent pas permettre l'identification des personnes concernées, et les travaux sur les données ne doivent pas aboutir à la promotion de produits en direction des professionnels de santé ou d'établissements de santé, ni permettre l'exclusion de garanties des contrats d'assurance ou la modification de cotisations ou de primes d'assurance.

L'accès aux données, s'il est par principe libre, est cependant soumis à l'obligation de présenter une demande d'accès aux données, auprès de l'Institut National des Données de Santé (INDS), devenu « Health Data Hub » en 2019[151]. Le protocole de l'étude portant sur les données devra être validé par un comité scientifique, existant soit au sein du Health Data Hub, soit aux seins des entrepôts de données locaux. La CNIL, enfin, se prononcera sur le respect du droit à la vie privée des personnes concernées.

Reste que, le principe d'open data s'appliquant, la mise à disposition des données de santé anonymisées doit se faire à titre gratuit. Les données étant produite à l'occasion d'une mission de service public, financée par l'impôt, elles seraient donc déjà payées. Ce principe viendrait donc s'opposer à la possibilité d'une valorisation à titre onéreux des données de santé dont disposent les

[150] Loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé

[151] Loi n° 2019-774 du 24 juillet 2019 relative à l'organisation et à la transformation du système de santé

hôpitaux, ce qui pourrait compromettre, incidemment, leur valorisation sociale : dans un contexte financier restreint, les établissements de santé sont parfois dans l'impossibilité de créer les infrastructures et organisations indispensables à l'anonymisation et à l'ouverture de ces données. Mohamed Adnène TROJETTE, dans son rapport de 2013, explique la situation ainsi :

« Pourtant, pour divers motifs – besoin budgétaire, situation de monopole, vision patrimoniale des informations et de la ressource qui en est tirée, volonté de limiter la demande ou de protéger un écosystème existant –, une vingtaine de services publics administratifs ont institué ou maintenu des redevances de réutilisation. Cela traduit, dans certains cas, une réelle inquiétude de l'administration de ne pas être en mesure de satisfaire les réutilisateurs, en termes de qualité des données et du service, mais aussi une crainte que les informations ainsi communiquées ne soient réutilisées pour critiquer le service public. »[152] « En forte baisse depuis 2010 (2 33 % en deux ans), le produit des redevances est le plus souvent perçu dans le cadre d'une vente en gros ou en détail de données, plus rarement en contrepartie de prestations de service sur mesure. Bien que, par ailleurs, les entités considérées contribuent parfois à la politique d'ouverture des données publiques, les modèles économiques de ces redevances ont pour effet d'en limiter les réutilisations. Ainsi, les tarifications retenues, souvent dégressives, tendent à cantonner l'accès aux acteurs établis ou ayant déterminé a priori les usages prévus. De ce fait, les acteurs moins dotés (citoyens, étudiants, chercheurs ou jeunes pousses, par exemple) sont exclus par ces barrières à l'entrée. Cette situation est préjudiciable, au regard des gains attendus d'une politique d'ouverture des données publiques, dont la vocation est la fourniture d'un bien public, vecteur d'externalités positives. Cela est d'autant plus préjudiciable qu'il s'agit souvent de jeux de données utiles à l'exercice de la démocratie et de

[152] TROJETTE Mohamed Adnène, « Ouverture des données publiques. Les exceptions au principe de gratuité sont-elles toutes légitimes ? », rapport au Premier Ministre, juillet 2013.

jeux de données à fort potentiel socioéconomique tels que les données géographiques, les données météorologiques ou les données de santé. »[153]

Il s'agit donc, dans un contexte où les aspects économiques comme sociaux sont particulièrement importants, de trouver un équilibre entre le droit à l'information et le droit au respect de la vie privée, mais également entre le droit à l'information et le respect des droits de propriété.

[153] Ibidem

Section 2 : La possibilité d'une valorisation des données de santé

Le principe de gratuité a longtemps été consacré de manière floue, sans être clairement établi. La loi CADA de 1978 prévoyait, à son article 15, que la réutilisation pouvait « donner lieu au versement d'une redevance », afin de couvrir les coûts d'anonymisation, les coûts de collecte, de production et de mise à disposition des informations, mais aussi pour permettre une rémunération raisonnable des investissements de l'administration, comprenant « le cas échéant, une part au titre des droits de propriété intellectuelle » et fut confirmée par le décret du 26 mai 2011[154], qui dispose qu'un décret fixerait limitativement la liste des informations soumises à redevance.

La loi du 28 décembre 2015 sur la réutilisation des informations prévoit cependant que « la réutilisation d'informations publiques est gratuite » en principe.

Le droit des personnes publiques vis-à-vis des données publiques est cependant apparu central à l'heure de la « République numérique » et de l'open data[155], et à l'heure de la valorisation du patrimoine immatériel des personnes publiques[156]. Si, autrefois, les droits de l'administration sur ces données publiques étaient incertains[157], les évolutions juridiques et organisationnelles ont permis de redonner une certaine maitrise de ces données par les personnes publiques.

---

[154] Décret n° 2011-577 du 26 mai 2011 relatif à la réutilisation des informations publiques détenues par l'Etat et ses établissements publics administratifs.

[155] YOLKA Philippe, « Open Data : L'ouverture, c'est l'aventure », *AJDA*, 2016, p. 76.

[156] LAJOUS Jacques, ROUSSEAU Christelle, « La valorisation du patrimoine immatériel des personnes publiques », Institut Universitaire de Varenne, LGDJ, Collection Colloques et Essais, janvier 2019.

[157] DUBAIL Charles-Henry, « Des données publiques à la propriété incertaine, LEGICOM, 2, n°25, p.160, 2001.

En 2013, le rapport « Bras » sur la gouvernance et l'utilisation des données de santé[158] exposait clairement une distinction entre les données de santé anonymes, soumises au principe d'Open Data, et les données nominatives et indirectement nominatives (anonymisées), ces dernières étant sujettes à un risque de réidentification indirecte, auxquelles l'accès est donc restreint. Cette logique sera reprise dans la loi de 2015 mentionnée auparavant.

Le rapport mentionnait également que l'accès aux données anonymes devrait se faire sans restriction, sans distinction d'usage ni de statut (public ou privé), contrairement aux données indirectement nominatives (données du SNIIRAM-PMSI…), soumises à un régime plus protecteur et introduisant l'idée d'une mise à disposition à titre payant et conditionnée par une transparence, une traçabilité et une finalité d'intérêt général[159].

Il apparait donc que les données de santé anonymes ou indirectement nominatives seules peuvent être considérées pour une potentielle valorisation – économique ou sociale. Celles-ci sont également soumises au principe d'Open Data, lequel peut sembler compromettre, du fait de la gratuité qu'il implique, la mise à disposition effective des données : la fourniture de données de qualité requérant des compétences des infrastructures techniques multiples et coûteuses, celle-ci peut être empêchée pour des enjeux de faisabilité économique pour certaines administrations publiques, dont les hôpitaux.

---

158 BRAS Pierre-Louis, « Rapport sur la Gouvernance et l'Utilisation des données de santé », remis à la ministre en chargé de la santé en Septembre 2013.

159 ROCHE Thomas, « Open data, Ouverture des données de santé », *Expertises* (*des systèmes d'information*), n°410, Février 2016, p. 59.

Aussi, la valorisation sociale des données de santé apparait effectivement possible si elle s'accompagne d'une valorisation économique : il s'agit de financer la mise à disposition des données de santé pour la rendre possible.

Des limites juridiques au principe d'ouverture des données à titre gratuit ont donc été posés afin, la plupart du temps, d'exprimer la réalité d'enjeux économiques[160]. Ceux-ci tiennent notamment en la valorisation de droits de propriété intellectuelle, mais également en la possibilité, pour un établissement de santé public, de fournir une prestation de service.

Tout d'abord, les droits de propriété intellectuelle (cf : Partie 1) peuvent emporter des droits à l'exclusivité sur la réutilisation des données[161].

Si un agent public peut être titulaire de droits d'auteur[162], dès lors qu'il créée une base de données, l'administration dont il dépend est titulaire du droit d'exploitation de l'œuvre[163]. L'exploitation commerciale de l'œuvre requiert cependant un intéressement de l'agent auteur[164], mais aucun décret n'est venu permettre la mise en œuvre de cet intéressement, lequel est, dans les faits, souvent occulté, tout du moins problématique[165].

[160] CLUZEL METAYER Lucie, « Les limites de l'Open Data », AJDA 2016, p.102.

[161] BERNAULT Carine, « Ouverture des données publiques et propriété intellectuelle », *Dalloz IP/IT*, p.103, Février 2018.

[162] Article L111-1 CPI

[163] Article L131-3-1 CPI

[164] Article L131-3-1 CPI

[165] L'auteur entend fonder son propos sur son expérience.

L'administration peut également, à la condition de fournir un investissement financier, matériel et humain substantiel, faire valoir un droit sui generis sur la base de données créée grâce à cet investissement[166], et donc en restreindre la réutilisation. Le juge administratif avait confirmé cette possibilité en 2015[167] : compte tenu de l'investissement réalisé, le département de la Vienne a été considéré comme le producteur de la base de données et pouvait exclure une réutilisation de celle-ci.

Dès lors, l'administration peut soumettre la réutilisation de données de santé anonymisées à la condition du paiement d'une redevance (éventuellement modulable) pour l'obtention d'une licence.

De plus, bien que les pouvoirs publics ne soient actuellement pas favorables à l'intervention d'établissements publics dans le champ économique, les établissements publics de santé « peuvent, à titre subsidiaire, assurer des prestations de service, valoriser les activités de recherche et leurs résultats et exploiter des brevets et des licences dans le cadre de services industriels et commerciaux.

Les centres hospitaliers universitaires peuvent prendre des participations et créer des filiales pour assurer des prestations de services et d'expertise au niveau international, valoriser les activités de recherche et leurs résultats et exploiter des brevets et des licences, dans des conditions et limites fixées par décret en Conseil d'État. »[168].

Au surplus, la réalisation de ces activités économiques ne doit pas porter préjudice à l'exercice de leurs missions.

---

166 Article L341-1 CPI

167 CAA Bordeaux, 26 février 2015, n°13BX00856.

168 Article 6145-7 CSP

A l'hôpital, les données de santé peuvent notamment être utilisées dans le cadre de la recherche, laquelle peut être réalisée dans l'intérêt général (santé publique, amélioration des connaissances médicales…) ou en partenariat avec un acteurs académique ou industriel.

Dans ce cadre, les activités économiques subsidiaires peuvent tenir en une prestation de recherche, un contrat de valorisation, etc. Cependant, l'établissement doit, pour cette activité, tenir une comptabilité analytique et respecter le principe de transparence des coûts[169], afin de ne pas facturer un coût inférieur au coût de revient de la prestation[170]. Enfin, l'activité doit être développée dans la limite des moyens humains et matériels indispensables à l'exécution des missions de service public des établissements publics de santé, être d'intérêt général et directement utile à l'établissement public[171].

Or, actuellement, il n'existe pas de mission du service public hospitalier correspondant précisément à la création de bases de données de santé et au traitement de ces données[172]. Il s'agit donc de justifier l'activité économique dans le cadre d'une autre mission de service public, notamment la mission de recherche, menée plus particulièrement au sein des Centre Hospitaliers Universitaires, lesquels apparaissent ainsi comme plus adaptés à la valorisation des données de santé.

D'autre part, il s'agit de déterminer un prix pour la prestation de service qui soit à la fois suffisamment élevé pour ne pas être inférieur au coût de revient de la prestation (et pouvant potentiellement tenant compte de la valeur réelle des données pour l'utilisateur, au regard des avantages de toute nature que l'accès aux données lui procure), et suffisamment bas afin de

---

169 Article R6145-7 CSP

170 Cette comptabilité analytique n'est pas toujours parfaitement mise en place pour les prestations de service en matière de recherche.

171 CAA Bordeaux 25 novembre 2003.

172 Article L6112-1 CSP

maintenir le principe de l'open data et ne pas freiner le développement économique et social que cette politique promet. Un prix trop élevé, injustifié, freinerait en effet les entreprises innovantes ayant recourt aux données de santé.

Un prix de marché doit donc être déterminé. Cependant, la détermination de ce prix reste complexe, et beaucoup d'établissements tâtonnent afin de trouver un juste prix pour leurs données. Des initiatives nationales, partenariales (Health Data Hub, Alliance Aviesan…) naissent ainsi afin de mener des réflexions ayant pour objet la détermination de la valeur économique de ces données de santé.

Bien que ces réflexions soient encore en cours, des pistes ont été proposées[173]. Ainsi, certains proposent des solutions de compromis, avec modulation des redevances suivant le type d'utilisateur (académique ou industriel) et la valeur ajoutée de l'offre (nature de la prestation de service et qualité des données…). La gratuité pourrait être assurée pour les citoyens et les entreprises de type « start-up », tandis que les entreprises de taille importante (Google, Microsoft…) auraient, elles, à payer un prix d'accès aux données. L'utilisation d'un système de double licence (licence ouverte et licence « partage à l'identique » / « share-alike ») est également préconisée afin de garantir que les données restent des biens communs, tout en permettant l'identification de la source des données.

Le domaine de la valorisation du patrimoine immatériel des personnes publiques, des bases de données possédées par les établissements de santé, reste cependant en construction, et la valorisation est aujourd'hui considérée comme insuffisante, bien qu'elle soit indispensable.

---

[173] Par exemple :

- CLUZEL METAYER Lucie, « Les limites de l'Open Data », AJDA 2016, p.102.
- TROJETTE Mohamed Adnène, « Ouverture des données publiques. Les exceptions au principe de gratuité sont-elles toutes légitimes ? », rapport au Premier Ministre, juillet 2013.

Titre 2 : La valorisation des données de santé au sein du Service Public Hospitalier : une pratique nécessaire à développer

La valorisation des données de santé au sein du Service Public Hospitalier se trouve remise en question au prisme de la nature publique de l'administration hospitalière, qui, soumise au principe de l'ouverture des données, ne devrait pas valoriser économique ce patrimoine immatériel prometteur, et qui au prisme de ses missions et des conditions de réalisation d'activités économiques subsidiaire doit trouver un passage étroit afin de pouvoir envisager une telle valorisation. Le sujet de la valorisation apparait dès lors flou.

Pourtant, nous venons de le voir, celle-ci semble possible. Malgré cela, le sujet de la valorisation au sein des établissements publics de santé apparait comme insuffisamment développé au sein des établissements de santé, bien qu'indispensable (Chapitre 1). Cette situation s'explique en partie par les organisations et structures indispensables à la mise en place de cette valorisation, encore trop embryonnaires dans les établissements publics de santé (Chapitre 2).

Chapitre 1 : La valorisation des données de santé, une nécessité insuffisamment mise en œuvre.

Section 1 : Ne pas valoriser n'est pas éthique

Il serait possible d'imaginer, pour des raisons de sécurité et afin d'éviter toute prise de risque, de ne pas procéder à la valorisation des données de santé. Cependant, l'insuffisance du recours au numérique et de la valorisation des données de santé, dans le cadre des activités de diagnostic, de soins ou de recherche, ou encore de pilotage du système de santé et des établissements qui le composent, induit des situations non-éthiques au sein de notre système de santé.

Pierre Delmas-Goyon, conseiller honoraire à la Cour de cassation, résume cette situation de la manière suivante : «On surfe entre deux écueils, explique-t-il, d'un côté ne pas se priver des innovations technologiques, ce qui serait non-éthique, et de l'autre côté le faire sans pour autant risquer de sacrifier des principes éthiques»[174].

Cette problématique était déjà exprimée dans l'avis 129 du CCNE en 2018. Le CCNE identifiait, alors, divers enjeux éthiques liés aux données de santé et à leur valorisation et aux différentes étapes de celle-ci.

Tout d'abord, le Comité identifiait une opposition de valeur entre le respect de la vie privée et la contribution à l'avancée des connaissances : la décision de mettre ses données de santé à disposition est personnelle, mais impacte la communauté, notamment dans le cadre de maladies

[174] MASCRET Damien, « Comment protéger les données médicales », Le Figaro, 29 mai 2019. http://www.lefigaro.fr/sciences/comment-proteger-les-donnees-medicales-20190529

rares[175]. Il identifiait par la suite une conciliation parfois complexe entre l'autonomisation des patients, leur capacité à maîtriser le devenir de leurs données (utilisation et réutilisation), avec l'intérêt collectif potentiel du traitement de ces données. De même, une conciliation s'avère nécessaire entre le principe du recueil du consentement des patients et le besoin de souplesse dans la mobilisation des données, dans le cas de la constitution d'entrepôts de données de santé au sein de certains établissements.

La valorisation de la donnée permettrait de développer la recherche, notamment pour les maladies rares où les traitements, comme les données, font défaut. Ce serait également « un moyen d'accélérer le développement de nouveaux traitements et de suivre leurs effets, en introduisant pour la première fois un échange équitable, numérisé et sécurisé entre patients, recherche pharmaceutique et autorités de santé. »[176]

La sécurité des interactions entre les niveaux locaux et nationaux (Health Data Hub) est également un enjeu majeur dans cette situation.

Au regard des différents travaux menés, il apparait qu'une néanmoins qu'une modalité d'action doit être dégagée afin de garantir le partage des données de santé, pour renforcer la qualité des soins et l'efficience du système de santé, tout en garantissant le respect des droits et libertés des personnes et la protection des données de santé.

Cette action qui doit être menée en faveur de la valorisation des données de santé se comprend premièrement du fait d'une concurrence particulièrement importante actuellement dans ce domaine. En effet, les grandes entreprises privées du secteur (GAFAM américaines, BATX

---

[175] AYME Ségolène, « Renforcement de la protection des données de santé : une menace et une opportunité pour les registres et cohortes dans le domaine des maladies rares », *La revue de médecine interne*, 2018, n°39, pp. 769-771.

[176] Le Monde, « Inventer un droit patrimonial sur les données de santé », 12 janvier 2019, p.7.

asiatiques…), ainsi que certains Etats comme les Etats-Unis, la Chine ou Israël, participent vivement à la valorisation des données de santé et au développement de technologies numériques – d'intelligence artificielle… –[177]. Les données que ces institutions sont amenées à capter, utiliser et sur lesquelles elles fondront le développement de leurs technologies peuvent provenir, en théorie et, parfois, en pratique, des données de citoyens français.

Cette situation pose de nombreuses questions éthiques : les données « françaises » récoltées à l'étranger ne sont pas soumises au droit français, et le cadre de leur utilisation n'est donc pas assurément éthique ou conforme aux exigences des français. D'autre part, économiquement, cette fuite de données peut désavantager la France dans la course à la technologie, et amener les financements français à être redirigés vers l'étranger. Enfin, les citoyens français auront certainement recours aux premières technologies produites par l'étranger, comme c'est actuellement le cas avec, par exemple, l'entreprise 23andme, entreprise de séquençage de génome américaine, ou l'entreprise israélienne MyHeritage, vers lesquelles de nombreux français se tournent, et auxquelles ils donnent accès à leurs données, sans bénéficier des garanties du droit français. De même, par exemple, Microsoft a obtenu, en Novembre 2018, la certification d'hébergeur de données de santé : les données tendent à migrer vers des plateformes gérées par des prestataires privés, et non-plus uniquement publics.

Le CCNE, dans son avis n°130[178], identifiait ce risque de « perte d'autonomie et de souveraineté », due à « un retard technologique dans les domaines de l'hébergement et du traitement de données ».

---

[177] STOEKLE Henri-Corto, VOGT Guillaume, « Nous devons « modifier nos normes de protection des données de santé » », Le Monde, 20 Juin 2019.

[178] Avis 130 du CCNE sur « Données massives (big data) et santé : une nouvelle approche des enjeux éthiques », paru le 28 mai 2019.

Au surplus, les technologies développées à l'étranger, avec des données de patients étrangers, pourraient ne pas être applicables à des patients français.

Il faut néanmoins noter la mise en place du Health Data Hub au niveau national, accompagnée par la constitution d'entrepôts de données de santé locaux, et soutenue par de nombreuses réflexions en matière de valorisation des données de santé (menées par la DREES, à travers un groupe de travail spécifique, ou encore par l'Alliance Aviesan, qui diligente des expertises…). Cette situation apparait suffisamment favorable, en pratique, au partage et à l'utilisation des données de santé, tout en garantissant une protection de celles-ci par le contrôle de leur partage, de préférence à travers du droit souple et par le développement de plateformes nationales mutualisées et interconnectées.

Cette politique devrait permettre à la France et à l'Europe de préserver leur autonomie stratégique et de ne pas perdre la maîtrise de la richesse que constituent les données de santé.

Section 2 : L'insuffisante valorisation des données de santé en France

La valorisation des données de santé peut être comprise sous deux aspects. Le premier de ces aspects consiste à valoriser les données en les partageant de manière large : c'est la politique d'ouverture des données. Le second aspect présente la valorisation des données de santé sous un angle plus économique et financier : il s'agit de percevoir un retour sur investissement au travers de la perception de redevances pour l'accès aux données.[179]

En 2007, l'Inspection Générale des Finances (IGF) et l'Inspection Générale de l'Administration de l'Éducation Nationale et de la Recherche identifiait la persistance d'un déficit de valorisation de la recherche publique et questionnait la suffisance des moyens accordés à cette mission de valorisation[180].

Le rapport identifiait, entre autres, le manque de réflexion et d'action commune en matière de valorisation : les structures de valorisation sont souvent propres à un établissement, les échanges de toutes natures (compétences…) entre structures sont faibles et il n'existe pas de politique partagée ambitieuse, malgré l'existence du Réseau C.U.R.I.E.. Au contraire, une concurrence néfaste existerait entre les différentes structures de valorisation.

---

[179] TERNEYRE Philippe, « Les actifs immatériels des personnes publiques », *Revue juridique de l'économie publique*, n°714, Décembre 2013, étude 16.

[180] « La valorisation de la recherche », Rapport IGAENR - Rapport conjoint I.G.A.E.N.R.-I.G.F. - janvier 2007.

Au surplus, les CHU ne sont pas directement partenaires des SATT (Sociétés d'Accélération du Transfert de Technologies). Il faudrait donc penser un modèle d'optimisation de la valorisation des données de santé, de la recherche[181].

A l'échelle internationale, des pays comme le Danemark, les États-Unis, le Canada ou Singapour, ont réussi à mettre en place un système efficace de valorisation de leurs données de santé, notamment à travers une politique d'open data en santé pensée de manière complète et fine, afin de valoriser les données de façon plus ambitieuse[182]. La réussite de ces initiatives semble ainsi reposer sur plusieurs fondements.

Tout d'abord, une volonté politique forte doit être exprimée afin de soutenir la politique d'ouverture des données. Cette volonté politique doit s'accompagner d'une structuration des bases de données de santé, à travers l'organisation des systèmes de collecte, de numérisation et d'agrégation des données de santé. Cette structuration est d'autant plus facilitée qu'une institution publique existe, en charge de la centralisation des données de santé. Enfin, un cadre réglementaire doit être mise en place afin de favoriser cette valorisation.

La mise en place d'un tel système a ainsi permis, dans ces pays, d'amorcer une valorisation des données de santé de manière effective.

En France, ces différents critères de réussites semblent aujourd'hui alignés (Health Data Hub, loi de modernisation de notre système de santé de 2016, loi relative à l'organisation et à la

[181] DELMOTTE Alexandre, « Les aspects juridiques de la valorisation de la recherche », *Mare & Martin*, Bibliothèque des thèses, Droit public, 2015.

[182] DREES, "Open data en santé : panorama international », janvier 2014.

transformation du système de santé de 2019[183]…), mais demandent encore à être développés : la situation actuelle présente toujours un manque d'outils et de dispositifs à destination des professionnels pour mener à bien une valorisation ambitieuse.

Au sein de l'hôpital public, la valorisation de la recherche pourrait passer, en partie, par la valorisation des données de santé, qui permettrait l'accroissement des recettes allouées à la recherche, si tant est que celles-ci ne soient pas excessives.

[183] LOI n° 2019-774 du 24 juillet 2019 relative à l'organisation et à la transformation du système de santé

Chapitre 2 : La valorisation des données de santé et la gestion publique

Section 1 : La valorisation des données de santé et la nouvelle gestion publique, d'une volonté à une nécessité

Au-delà des volontés politiques de développer la valorisation (économique et sociale) des données, notamment des données de santé, et des traductions juridiques de ces volontés, il apparait que la valorisation des données publiques, dont les données de santé, soit indispensable.

En effet, selon certains auteurs, la valorisation des données, passant en principe par une politique d'open data, pourrait générer une forte croissance économique en permettant une libération de l'innovation et un accroissement de la performance des administrations[184].

La valorisation économique des données se ferait notamment grâce à l'ouverture des données, qui conférerait à la France un atout concurrentiel majeur sur la scène internationale, en permettant l'émergence d'une économie numérique sur le territoire national. Au surplus, la réutilisation des données favorise autant l'initiative privée que la valorisation des propriétés

[184] MANYIKA J. et al., « Open data: unlocking innovation and performance with liquid information", rapport du McKinsey Global Institute, 2013.

publiques immatérielles, notamment à travers une collaboration renouvelée entre les acteurs publics, privés et la société civile[185] (co-innovation).

L'ouverture des données, étape fondamentale de la valorisation, permettrait également d'enclencher un cercle vertueux en dynamisant la valorisation du « portefeuille de droits immatériels »[186] des administrations, des hôpitaux. Si la gratuité reste le principe, la tarification doit être envisagée en cas de réutilisations commerciales ou d'investissement de la part de l'administration (plus-value apportée aux données accessibles de par leur indexation ou mise à jour) :

« Si l'objectif des politiques publiques est de diffuser des informations brutes, difficiles à comprendre et à utiliser pour le non-initié, alors il est optimal que ces informations soient gratuites. Mais si l'objectif est de faciliter la réutilisation en l'accompagnant et en diffusant des ISP enrichies en format et/ou en contenu, alors une tarification positive, raisonnable et calibrée financement en fonction du consentement à payer des utilisateurs, peut être optimale. Surtout, lorsque le budget des services publics producteurs d'ISP est contraint. A la limite, lorsque le savoir-faire permettant une meilleure compréhension et utilisation des ISP est également diffusé, il devient alors optimal de faire payer pour ce savoir-faire »[187].

On comprend ici qu'il est envisageable de proposer une tarification positive pour les données de santé, et que les recettes tirées de cette valorisation pourront par la suite nourrir des investissements en infrastructures, en compétences, en savoir-faire, afin de proposer un service d'accès aux données

---

185 BOURCIER D., de FILIPPI P., « Vers un nouveau modèle de service commun entre l'administration et les communautés numériques », Génération Y et gestion publique : quels enjeux ?, MATYJASIK N., MAZUEL P. (Ed.), 2012.

186 JOUYET Jean-Pierre, LEVY Maurice, « L'économie de l'immatériel : la croissance de demain », Rapport pour le ministre de l'économie, des finances et de l'industrie, décembre 2006.

187 Bureau d'économie théorique et appliquée, « La valorisation des informations du secteur public : un modèle économique de tarification optimale, rapport final », décembre 2010.

toujours meilleur. Il faut néanmoins veiller à ce que la redevance ne devienne pas excessive, ayant pour objet strict l'augmentation des recettes financières de l'établissement. Celle-ci doit se cantonner à des recettes marginales, suffisante pour couvrir les coûts de fonctionnement et d'éventuels investissements.

D'autre part, l'open data permettrait un gain démocratique majeur, en permettant un contrôle des activités et des actions de la puissance publique, pouvant aller jusqu'à l'évaluation des politiques publiques menées ou envisagées afin d'interroger leur efficience, leur pertinence. En cela, l'open data apparait comme un outil de performance particulièrement utile dans le contexte de la Nouvelle Gestion Publique[188].

La transparence apparait en effet comme un moyen de garantir l'efficience et l'efficacité de l'action publique[189]. Dans le cadre de la nouvelle gestion publique, la RGPP puis la MAP ont promu le recours au numérique et l'ouverture des données afin de transformer et de moderniser l'action publique : l'administration contrôlée et évaluer est amenée à améliorer son fonctionnement, améliorant ainsi la qualité du service public rendu à l'usager.

Les données publiques ouvrent ainsi la porte à l'approfondissement du débat démocratique tout en portant la promesse d'une création de valeur économique majeure, chose relativement rare dans l'histoire.

Ainsi, pour les établissements de santé, la valorisation des données de santé, à travers la mise au point de technologies d'IA ou à travers l'évaluation des données, permettrait d'améliorer

---

188 LOVELUCK Benjamin, « Vers une économie politique des données : le pouvoir à l'aune des data », in BOURCIER, Danièle et DE FILIPPI Primavera (dir.), « Open data & Big data ; Nouveaux défis pour la vie privée », *LGDJ*, Éditions Mare et Martin, pp. 245-262

189 MARCHAND Jennifer, « L'open data, la réutilisation des données publiques entre exigence démocratique et potentiel économique », *JCP A.*, 17 févr. 2014, n° 7, p. 2038

la gestion de l'établissement, à travers l'optimisation des protocoles de soins (aide au diagnostic, aide au choix du protocole de soin, pharmacovigilance, suivi de l'observance des traitements, identification des personnes à risques), la facilitation de la recherche (identification simplifiée de patients correspondant au protocole d'inclusion d'un essai clinique, simplification de la réalisation d'étude observationnelle), l'appui au pilotage médico-économique (identification de politiques adaptées, de tendances de santé publique, de l'offre de soins sur le territoire, aide à l'évaluation interne et externe…).

Section 2 : La gouvernance nécessaire à la valorisation des données de santé

La valorisation des données de santé requiert une organisation ainsi qu'une gouvernance spécifique, propre à l'objet complexe que constitue le big data en santé.

La qualité de la gouvernance des données apparait comme un facteur clef de la valorisation[190] : il s'agit, afin de réaliser une valorisation efficace, de structurer les données et d'organiser leur traitement, mais également l'ensemble des processus de valorisation (notamment les processus administratifs et juridiques) de manière à garantir et maximiser leur qualité et leur valeur.

Ainsi, nous l'avons vu plus tôt, la sécurité des données prend une importance majeure.

[190] MONINO Jean-Louis, SEDKAOUI Soraya, « Big data, Open data et valorisation des données », ISTE éditions, série Smart Innovation, 2016.

Celle-ci est notamment assurée par le DPO (Data Protection Officer, ou Délégué à la Protection des Données, DPD en français)[191], qui met en place un suivi et une évaluation des processus mis en place et est associé à toutes les questions relatives à la protection des données personnelles. Cet acteur est obligatoirement désigné lorsque le traitement des données est effectué par une autorité publique ou un organisme public et peut être mutualisé.

Le DPO est avant tout un auditeur de la conformité réglementaire des traitements, et en cela il doit disposer d'une expertise juridique et technique en matière de protection des données personnelles, bien connaître son secteur d'activité et l'établissement et ses besoins pour lequel il est missionné.

Une fois la sécurité des données assurée, la garantie de leur qualité est indispensable. Celle-ci repose notamment sur des ingénieurs, *data scientists*, médecins (ayant des connaissances ou une spécialité en information médicale) capable de nettoyer, d'intégrer et de transformer les données afin de leur conférer une qualité importante, et ainsi de maximiser leur valeur.

La qualité des données est particulièrement indispensable lorsqu'elles sont utilisées dans un processus décisionnel, dans le cadre du pilotage d'un établissement de santé ou du système de santé par exemple. Les données se doivent alors d'être précises et sûres. Transposé au secteur public, le concept d'« Intelligence économique » apparait également pertinent, afin de contribuer à orienter, modifier, améliorer les activités d'un établissement, les politiques de santé, afin de les rendre plus pertinentes, plus adéquates, plus efficaces, au service de l'usager.

Enfin, les processus juridiques et administratifs qui entourent la valorisation des données (contractualisation, réponse à des appels à projets, création de partenariats…) doivent également

[191] CHAPEL Elodie, GRUSON David et alli., « La révolution du pilotage des données de santé. Enjeux juridiques, éthiques et managériaux », LEH Edition, Décideur santé, Juin 2019.

être optimisés afin de maximiser la valorisation – économique comme sociale – des données de santé. Dans ce cas, il importe de recourir à des juristes, assistants de recherche clinique, etc… qualifiés, afin de garantir la qualité de ce processus.

Ces différentes compétences – DPO, ingénieur, juristes… - sont donc indispensables afin de permettre une valorisation ambitieuse des données de santé au sein du service public hospitalier. Cependant, ces compétences sont souvent coûteuses et/ou rares, et les moyens, notamment financiers, à disposition des établissements de santé afin d'attirer ces compétences et talents, sont restreints.

Notamment, le plafonnement des rémunérations apparait comme un frein à l'attractivité de l'hôpital.

Conclusion

Il apparait qu'après de nombreuses réflexions éthiques, juridiques et économiques, la valorisation des données de santé soit non-seulement devenue possible, mais également indispensable.

Elle permettrait, globalement, l'amélioration du système de santé, à travers l'amélioration des connaissances médicales, la mise au point de nouvelles technologies médicales, l'amélioration de la gestion hospitalière, etc…

Au surplus, cette valorisation des données de santé, qui revêt un intérêt à la fois social et économique, s'avère conciliable, sous certaines conditions, avec le respect des droits des personnes concernées par les données, ainsi qu'avec le cadre juridique concernant la propriété intellectuelle, les activités économiques des établissements de santé, ou encore le droit public économique.

Cependant, la valorisation des données de santé repose sur des processus, des compétences, des infrastructures, un cadre juridique très spécifiques et complexes. Par certains aspects, la France apparait en retard dans certains de ces domaines, qui sont cependant en voie d'amélioration.

La création, en 2019, du Health Data Hub, apparait ainsi comme un véritable tournant pour la valorisation des données de santé, en tant qu'entité « leader » dans ce domaine. Il s'agira de transformer l'essai en réussite, afin de permettre à la France de rester compétitive dans ce domaine, et afin de faire valoir tous les atouts dont le pays dispose.

Bibliographie

Articles

- ABBOUB Schéhérazade, COQUEL Emilie, « Les modalités de mise à disposition des données publiques locales », *RFDA* 2018, p. 35.
- ANOHORY Michèle, CHU Robert, NORMAND Alexis, SPREUX Oliver, « Il faut inventer un droit patrimonial sur ses données de santé », tribune, *Le Monde*, 11 Janvier 2019.
- APPOLIS B., « Vers une transformation financière du système de santé ? », *RDSS*, 1/ 2019, p. 35.
- AUBY Jean-Bernard :
  - JurisClasseur Administratif, chap. « Données publiques », fasc. 109-30 et suivants, par J.B. AUBY et T. PIETTE-COUDOL, notamment :
    « Données publiques – Définitions. Principes. Orientation », *JurisClasseur Administratif*, fasc. 109-30, 10 Avril 2018 (révisé le 13 Novembre 2018) ;
    « Données publiques – Production interne et collecte sur le secteur privé », *JurisClasseur Administratif*, fasc. 109-40, 30 Novembre 2017 ;
    « Données publiques – Gestion Administrative et exploitation technique », *JurisClasseur Administratif*, fasc. 109-50, 30 Novembre 2017 ;
    « Données publiques – Publication. Réutilisation », *JurisClasseur Administratif*, fasc. 109-30, 24 Avril 2018 (révisé le 13 Novembre 2018).
  - « Le droit administratif face aux défis du numérique », *AJDA*, 2018, p. 835.
- AYME Ségolène, « Renforcement de la protection des données de santé : une menace et une opportunité pour les registres et cohortes dans le domaine des maladies rares », *La revue de médecine interne*, 2018, n°39, pp. 769-771.
- BABUSIAUX Christian, « L'ouverture de bases de données de données publiques : le point et les enjeux de santé *», I2D – Information, données et documents*, 2016/3 Volume n°53, pp. 48-50.
- BASSI Timothée, « Les données collectées par le concessionnaire de service public », *AJDA* 2019, p. 496.
- BEAUCHAMP T.L., CHILDRESS J.F., « Les principes de l'éthique biomédicale », *Médecine et Droit*, volume 2008, n° 89 (mars-avril 2008), p.59 (traduit de l'américain).

- BERANGER Jérôme, « La valeur éthique de la donnée de santé à caractère personnel : vers un nouveau paradigme de l'écosystème médical dématérialisé », *Sciences de la société*, 95 / 2016.
- BERGOIGNAN-ESPER C., « L'hôpital public au sein du plan « Ma santé 2022 », *RDSS* 1/ 2019, p. 15.
- BERNAULT Carine, « Ouverture des données publiques et propriété intellectuelle », *Dalloz IP/IT*, p.103, Février 2018.
- BICLET Philippe (Dr.), « Où en est-on du Big Data en médecine ? », *Médecine & Droit*, 2018, pp. 62-67.
- BOIZARD Maryline, « La valorisation des données numériques par la protection juridique des algorithmes », *Dalloz IP/IT*, 2018, n°02/2018, p.99.
- BORGETTO Michel, « Le plan "Ma santé 2022" », *RDSS* 2019, p. 03.
- BOUCHER Julien, BOURGEOIS-MACHUREAU Béatrice, « Redevances pour service rendu : l'assouplissement de la règle du plafonnement par le coût », commentaire sous Conseil d'Etat, Ass., 16 Juillet 2007, « Syndicat national de défense de l'exercice libéral de la médecine à l'hôpital », n°293229 293254, *AJDA*, 2007, p. 1807.
- BOUL Maxime, « Réflexions sur la notion de donnée publique », *RFAP*, 2018/3, n°167, pp. 471-478.
- BOURCIER Danièle, DE FILIPPI Primavera, « Transparence des algorithmes face à l'open data : quel statut pour les données d'apprentissage ? », *RFAP*, 2018/3, n°167, pp. 525-537.
- BOURCIER, Danièle et DE FILIPPI Primavera, (dir.) « Open data & Big data ; Nouveaux défis pour la vie privée », *LGDJ*, Éditions Mare et Martin, 270 p., 2016.
- BRAIBANT Guy, « Droit d'accès et droit à l'information », Mélanges Robert-Edouard Charlier, Ed. de l'Université, 1981.
- CAMUS Aurélien, « La propriété des données publiques », *RFAP*, 2018/3, n°167, pp. 479-490.
- CHEVALLIER Jacques, « Vers l'Etat-plateforme ? », *RFAP*, 2018/3, n°167, pp. 627-637.
- CLUZEL-METAYER Lucie,
  - « La construction d'un service public de la donnée », *RFAP*, 2018/3, n°167, pp. 491-500.
  - « La loi pour une République numérique : l'écosystème de la donnée saisi par le droit, *AJDA*, 2017, p.340.

- « Les limites de l'Open Data », AJDA 2016, p.102.

- CLUZEL-METAYER Lucie, DEBAETS Emilie, « Le droit de la protection des données personnelles : la loi du 20 juin 2018 », *RFDA* 2018, p. 1101.
- DAUTIEU Thomas, GABRIE Emile, « Analyse de l'apport de la loi pour une République numérique à la protection des données à caractère personnel (1ère partie) – L'ouverture de l'accès aux données publiques et sa conciliation avec la protection des données à caractère personnel », *Communication Commerce Electronique*, 2016, n°12, étude 22.
- DEBIES Elise, « Big data de santé et autodétermination informationnelle : quelle articulation possible pour une innovation protectrice des données personnelles ? », *RFAP*, 2018/3, n°167, pp. 565-574.
- DE FILIPPI Primavera, « La double face de l'Open Data », *Les petites affiches*, 2013, n°203, p. 6.
- DEMOTES-MAINARD Jacques, CORNU Catherine, GUERIN Aurélie, et alli. « Quel impact du nouveau règlement européen sur la protection des données sur la recherche clinique et recommandations », *Thérapies*, Vol 74 - N° 1 - février 2019, pp. 17-29. Numéro dédié aux XXXIVès Rencontres Nationales de Pharmacologie et Recherche Clinique, pour l'Innovation Thérapeutique et l'Évaluation des Technologies de Santé - Tables rondes Giens – 7 au 8 octobre 2018, organisées par la Société française de pharmacologie et de thérapeutique.
- DEROUDILLE Alexis, « Le secret professionnel dans le règlement général sur la protection des données », *RFDA* 2018, p. 1112.
- DESMARAIS Pierre, « Numérique - Informations publiques et données personnelles, quand la jurisprudence distingue enfin vie privée et droit des données - Etude par Pierre Desmarais », *Revue pratique de la prospective et de l'innovation*, 01 Octobre 2017.
- DIEBOLT Vincent, AZANCOT Isaac, BOISSEL François-Henri, et alli, « « Intelligence artificielle » : quels services, quelles applications, quels résultats et quelle valorisation aujourd'hui en recherche clinique ? Quel impact sur la qualité des soins ? Quelles recommandations ? », *Thérapies*, Vol 74 - N° 1 - février 2019, pp. 141-154. Numéro dédié aux XXXIVès Rencontres Nationales de Pharmacologie et Recherche Clinique, pour l'Innovation Thérapeutique et l'Évaluation des Technologies de Santé - Tables rondes Giens – 7 au 8 octobre 2018, organisées par la Société française de pharmacologie et de thérapeutique.
- DONNASSON Sylvie, « Le big data dans la santé : réalités et perspectives en France : big data, open data et smart data, applications, initiatives et enjeux stratégiques pour les acteurs

du système de santé », *Les Échos études*, étude réalisée en partenariat avec HealthInnov ; [rédigée par Sylvie Donnasson] ; [sous la direction d'Hélène Charrondière].

- DREYFUS Jean-David, « La valorisation par l'Etat de son patrimoine immatériel », *AJDA* 2009, p. 696.
- EON Florence, « L'accélération du numérique en santé : enjeux et conditions de son succès », *RDSS* 1 / 2019, p. 55.
- FALQUE-PIERROTIN Isabelle, « La CNIL face à l'économie de la donnée », *AJCA* 2016, p. 175.
- GABAYET Nicolas, « Open data et loi CADA : la primauté du droit de réutilisation des bases de données publiques sur le droit de propriété », *La Semaine Juridique Administrations et Collectivités territoriales*, 17 Octobre 2017, n°41, p. 2241.
- GRUSON David, La révolution du pilotage des données de santé - Enjeux juridiques, éthiques et managériaux », LEH Editions, mai 2019, 147 pages.
- ISAAC Henri, « La donnée numérique, bien public ou instrument de profit », *Pouvoirs*, 2018/1, n°164, pp. 75-86.
- JACQUET Marie-Anne, « Le virage numérique à l'hôpital : un processus de transformation globale », *Gestion et Finances Publiques*, n°1-2019, Janvier-Février 2019, pp. 37-43.
- JAREMKO Jacob L., AZAR Marleine, BROMWICH Rebecca et alli, « Canadian Association of Radiologists White Paper on Ethical and Legal Issues Related to Artificial Intelligence in Radiology », *Canadian Association of Radiologists Journal*, 70 (2019), pp. 107-118.
- KOUBI Geneviève, « Equivoque administrative de la notion de donnée publique », *La Semaine Juridique Administrations et Collectivités Territoriales*, n°18-19, 7 mai 2018, p. 2142.
- LAJOUS Jacques, ROUSSEAU Christelle, « La valorisation du patrimoine immatériel des personnes publiques », Institut Universitaire de Varenne, LGDJ, Collection Colloques et Essais, janvier 2019.
- LANNA Maximilien, « Données publiques et protection des données personnelles : le cadre européen », *RFAP*, 2018/3, n°167, pp. 501-511.
- LESAULNIER Frédérique, « Recherche en santé et protection des données personnelles à l'heure du Règlement général relatif à la protection des données », *Médecine & Droit*, 2018.
- LOVELUCK Benjamin, « Vers une économie politique des données : le pouvoir à l'aune des data », in BOURCIER, Danièle et DE FILIPPI Primavera (dir.), « Open data & Big data ; Nouveaux défis pour la vie privée », *LGDJ*, Éditions Mare et Martin, pp. 245-262.

- LUCAS Jacques, « Le partage des données personnelles de santé dans les usages du numérique en santé à l'épreuve du consentement exprès de la personne », *Ethics, Medicine and Public Health*, 2017, n°3, pp. 10-18.
- MAMZER Marie-France, HERVE Christian, « La requalification des données de soins en données de recherche : enjeux éthiques et normatifs », *Ethics, Medicine and Public Health*, 2017, n°3, pp. 83-89.
- MANYIKA J. et al., « Open data: unlocking innovation and performance with liquid information", rapport du McKinsey Global Institute, 2013.
- MANSON Stéphane, « La mise à disposition de leurs données publiques par les collectivités territoriales », *AJDA* 2016, p. 97.
- MARCHAND Jennifer, « L'open data, la réutilisation des données publiques entre exigence démocratique et potentiel économique », *JCP A*., 17 févr. 2014, n° 7, p. 2038.
- NANTEL Lyne, « Open data & Big data ; Nouveaux défis pour la vie privée, note de lecture », *Communiquer*, 2017, n°19, pp. 151-154.
- PECHILLON Éric, « L'accès ouvert aux données de santé : la loi peut-elle garantir tous les risques de dérives dans l'utilisation de l'information ? », *L'information psychiatrique*, 2015/8, Volume 91, pp. 645-649.
- PELLEGRINI François, « La portabilité des données et des services », *RFAP*, 2018/3, n°167, pp. 513-523.
- PEUGEOT Valérie, « Données de santé : contours d'une controverse », Alternatives économiques, L'économie politique, n°80, 2018, pp. 30-41
- PON Dominique, « Une approche raisonnée et progressive de la transformation numérique », *Techniques Hospitalières*, n°776, mai-juin 2019.
- RICHER Laurent, « L'hédonisme au Conseil d'Etat », *AJDA* 2007, p. 2057.
- ROBIN Agnès,
  - « La valorisation. Définition dans le contexte de la recherche scientifique », *Lex Electronica*, Université de Montréal, 2017*, Droit, sciences et techniques : des concepts aux régimes*, dir. E. Vergès, pp. 138-152.
  - « Les données scientifiques au prisme du dispositif open data », *Communication Commerce Électronique*, Lexis-Nexis, 2017, 9 (étude 14), pp. 7-14.
  - « Valorisation de la recherche scientifique, propriété intellectuelle, innovation », *Cahiers Droit, Sciences & Technologies*, 7 /2017, 205-221.

- « Valorisation de la recherche publique, innovation, propriété intellectuelle », *Cahiers Droit, Sciences & Technologies*, 4 / 2014, 251-258.

- ROCHE Thomas, « Open data, Ouverture des données de santé », *Expertises* (*des systèmes d'information*), n°410, Février 2016, p. 59.
- ROLLAND Louis, « Précis de droit administratif, » petit précis Dalloz, 1947, 9ème édition.
- SAISON Johanne, « Ma Santé 2022 : une nouvelle étape vers la consécration d'un service public de santé ? », *RDSS* 1/ 2019, p.25.
- SIRANYAN Valérie « La protection des données personnelles des patients face à la modernisation de notre système de santé », *Médecine et Droit* (Paris), 2018.
- SOL Hélène, « Big Data en santé : données concernées, usages, entrepôt bio-hétérogènes et outils d'exploitation (Avis d'experts) », *ANAP*, 07 Janvier 2016.
- TERNEYRE Philippe,
  - « Les actifs immatériels des personnes publiques », *Revue juridique de l'économie publique*, n°714, Décembre 2013, étude 16.
  - « Nouvelle détermination du montant des redevances pour service rendu », commentaire sous Conseil d'Etat, Ass., 16 Juillet 2007, « Syndicat national de défense de l'exercice libéral de la médecine à l'hôpital », n°293229 293254, *AJDA*, 2007, p. 1807.
- THEARD-JALLU Cécile, GOSSE Nina, « Hôpital 4.0 et IA : les défis juridiques », Techniques hospitalières, n°776, mai-juin 2019.
- THEARD-JALLU Cécile, GOSSE Nina, VUITTON Xavier, « Intelligence artificielle : quels défis juridiques pour vos partenariats entre la France et le Canada ? », Le Monde Juridique, Février 2019.
- VERDIER Henri, VERGNOLLE Suzanne, l'État et la politique d'ouverture en France, AJDA 2016, p. 92.
- VIOUJAS V., « La résurrection du service public hospitalier », AJDA, 2016, p. 1272.
- YOLKA Philippe, « Open Data : L'ouverture, c'est l'aventure », *AJDA*, 2016, p. 76.
- ZOLYNSKI Célia, « Un nouveau droit de propriété intellectuelle pour valoriser les données : le miroir aux alouettes ? », *Dalloz IP/IT* 2018, p.94.

Jurisprudences

- Conseil d'Etat, Ass., 16 Juillet 2007, « Syndicat national de défense de l'exercice libéral de la médecine à l'hôpital », n°293229 293254, publié au recueil Lebon.
- Conseil d'Etat, 10ème et 9ème chambres réunies, 8 Février 2017, « NotreFamille.com », n°389806.

Ouvrages généraux et spéciaux : manuels, monographies, thèses et travaux collectifs.

- AHNER Francis, TOUATI Jean-Jacques, « Inventions et créations des salariés », 2ème édition, *Lamy*, Collection Axe Droit.
- BENSOUSSAN Alain, « Informatique et libertés », 2ème édition, *Francis Lefebvre*, Paris, 2010.
- BITAN H., Droit des créations immatérielles (logiciels, bases de données, autres œuvres du Web 2.0), *Lamy*, Axe droit, 2010.
- CATALA Pierre, « Le droit à l'épreuve du numérique », *PUF*, 1998.
- CHAPUS, René. Droit administratif général, Tome 1, 15ème édition, Montchrestien, 2001.
- CORNU, Gérard. Vocabulaire juridique, PUF, 2015.
- DELAHAYE Jean-Paul, « Les blockchains, clefs d'un nouveau monde », Pour la Science, n° 449, pp. 80-85, Mars 2015.
- DELMOTTE Alexandre, « Les aspects juridiques de la valorisation de la recherche », *Mare & Martin*, Bibliothèque des thèses, Droit public, 2015.
- DUPONT Marc, BERGOIGNAN-ESPER, Claudine, PAIRE, Christian, « Droit hospitalier », *Dalloz*, 10éme édition, 2017.
- DUPUY Olivier, « La gestion des informations relatives au patient », *Les études hospitalières*, 2005.
- FERAL-SCHUHL Christiane, « Cyberdroit, le droit à l'épreuve de l'internet », 7ème édition, *Dalloz*, 2018-2019.
- FIESCHI Marius, DUFOUR Charles, « Traitement des données en santé, approches systémiques », *ISTE éditions*, Collection Santé, Technologies et Société, Série Industrialisation de la santé, Volume 9, mai 2018.
- GRUSON David, CHAPEL Elodie, « La révolution du pilotage des données de santé – Enjeux juridiques, éthiques et managériaux », LEH Edition, Mai 2019.

- HERVE Christian, STANTON-JEAN Michèle (dir.), « Innovations en santé publique, des données personnelles aux données massives (Big data) – Aspects cliniques, juridiques et éthiques », *Dalloz*, Thèmes et commentaires, Ethique biomédicale et normes juridiques, 2018.
- HERVE Christian, STANTON-JEAN Michèle, MARTINENT Eric (dir.), « Les systèmes informatisés complexes en santé – Banque de données, télémédecine : normes et enjeux éthiques », *Dalloz*, Thèmes et commentaires, Actes, 2013.
- LAUDE Anne, TABUTEAU Didier, « Droit de la santé », 3ème édition, *PUF*, 2012.
- MATTATIA Fabrice, « Droit d'auteur et propriété intellectuelle dans le numérique », *Editions Eyrolles*, août 2017.
- MONINO Jean-Louis, SORAYA Sedkaoui, « Big data, Open data et valorisation des données », *ISTE éditions*, Collection Innovation, Entrepreneuriat et Gestion, Série Smart Innovation, Volume 4, Février 2016.
- MOQUET-ANGER Marie-Laure, « Droit Hospitalier », 5ème édition, *Dalloz*, 2018.
- NETTER Emmanuel (dir.), CHAIGNEAU Aurore (dir.), « Les biens numériques », CEPRISCA, Collection Colloques, 2015, 242 pages.
- ROCHFELD Judith, « Contre l'hypothèse de la qualification des données personnelles comme des biens », in Les biens numériques, éditions CEPRISCA, pp. 221-236, 2015.
- SAISON-DEMARS Johanne, « Droit hospitalier », 3ème édition, *Gualino*, 2011.

Thèses et Mémoires

- AIT MOUHOUB LOUALI Nadia, « Le service public à l'heure de l'Open Data. », thèse de doctorat soutenue le 28 Juin 2018 à Paris 2.
- OUMEDJKANE Antoine, « Compliance et Droit Public », mémoire de recherche de Master 2, Faculté de Droit et de Science Politique de Montpellier, 2018, récompensé par le « Prix de l'AFDA récompensant le meilleur mémoire de recherche de master 2 ».
- CAVALIER, Mathilde. La propriété des données de santé, thèse Lyon, 2016.

Avis, Etudes et Rapports

- Administrateur Général des données (2015), Rapport au Premier Ministre, sur La gouvernance de la donnée, « Les données au service de la transformation de l'action publique ».
- Administrateur Général des données (2018), Rapport au Premier Ministre, 2016-2017, « La donnée comme infrastructure essentielle ».
- ADNOT Philippe, Rapport d'information n° 341 (2005-2006), « La valorisation de la recherche dans les universités : une ambition nécessaire », fait au nom de la commission des finances, déposé le 10 mai 2006.
- BRAIBANT Guy, « Données personnelles et société de l'information – Rapport au Premier Ministre sur la transposition en droit français de la directive n°95/46 », 3 mars 1998.
- BRAS Pierre-Louis, LOTH André, « La gouvernance et l'utilisation des données de santé », septembre 2013.
- CCNE Avis 129, « Contribution du Comité consultatif national d'éthique à la révision de la loi de bioéthique 2018-2019 », adopté le 18 septembre 2018.
- Comité Consultatif National d'Ethique (CCNE), Avis n°130, « Données massives et santé : une nouvelle approche des enjeux éthiques », avis rendu public le 29 mai 2019.
- Commission Nationale Informatique et Liberté (CNIL), Commission d'Accès aux Documents Administratifs (CADA) et Etalab, « Guide pratique de la publication en ligne et de la réutilisation des données publiques – "Open data" ».
- Conseil d'Etat (2014), « Le numérique et les droits fondamentaux », *Etudes et documents*, n°65, La documentation Française.
- Conseil d'Etat (2017), « Puissance publique et plateformes numérisées. Accompagner l'ubérisation », *Etudes et documents*, n°68, La documentation Française.
- Cour des Comptes, « Les données personnelles de santé gérées par l'assurance maladie - une utilisation à développer, une sécurité à renforcer », communication à la commission des affaires sociales et à la mission d'évaluation et de contrôle des lois de financement de la sécurité sociale de l'Assemblée nationale, mars 2016.
- CUGGIA Marc, POLTON Dominique, WAINRIB Gilles, COMBES Stéphanie, Rapport « Health Data Hub – Mission de préfiguration », Ministère de la Santé et des Solidarités, Octobre 2018, 110 pages.

- FOUILLERON Antoine, « Les échanges de données réalisés à titre onéreux entre les administrations – Rapport au Premier ministre », novembre 2015.
- TROJETTE Mohamed Adnène, « Ouverture des données publiques. Les exceptions au principe de gratuité sont-elles toutes légitimes ? », rapport au Premier Ministre, juillet 2013.
- VILLANI Cédric, Rapport « Donner du sens à l'Intelligence Artificielle : pour une stratégie nationale et européenne », 28 mars 2018, La documentation Française, 235 pages.
- VILLANI Cédric, LONGUET Gérard, « Rapport au nom de l'Office Parlementaire d'Evaluation des Choix Scientifiques et Technologiques sur l'Intelligence Artificielle et les Données de Santé », OPECST, 21 mars 2019.

Lois et Règlements

Lois

- Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.
- 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, dite « loi CADA ».
- 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.
- Loi n° 82-610 du 15 juillet 1982 d'orientation et de programmation pour la recherche et le développement technologique de la France, dite « loi Chevènement », JORF du 16 juillet 1982 page 2270.
- Loi n° 83-634 du 13 juillet 1983 portant droits et obligations des fonctionnaires. Loi dite « loi Le Pors ».
- Loi n° 86-33 du 9 janvier 1986 portant dispositions statutaires relatives à la fonction publique hospitalière.
- Loi n° 99-587 du 12 juillet 1999 sur l'innovation et la recherche, dite « loi Allègre », JORF n°160 du 13 juillet 1999 page 10396.
- Loi n° 2000-321 du 12 Avril 2000 relative aux droits des citoyens dans leurs relations avec les administrations.
- Loi n°2004-810 du 13 Août 2004 relative à l'Assurance-maladie.

- Loi n°2009-879 du 21 juillet 2009 portant réforme de l'hôpital et relative aux patients, à la santé et aux territoires, dite « Hôpital, patients, santé et territoire » ou « HPST ».
- Loi n° 2012-300 du 5 mars 2012 relative aux recherches impliquant la personne humaine, dite « loi Jardé », JORF n°0056 du 6 mars 2012 page 4138.
- Loi n° 2015-990 du 6 août 2015 pour la croissance, l'activité et l'égalité des chances économiques.
- Loi n° 2015-1779 du 28 décembre 2015 relative à la gratuité et aux modalités de la réutilisation des informations du secteur public.
- Loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé.
- Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique et Exposé des motifs - Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique.
- Loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles.
- Loi n° 2019-774 du 24 juillet 2019 relative à l'organisation et à la transformation du système de santé.

Décrets

- Décret n°2005-1755 du 30 décembre 2005 relatif à la liberté d'accès aux documents administratifs et à la réutilisation des informations publiques, pris pour l'application de la loi n° 78-753 du 17 juillet 1978.
- Décret n° 2009-151 du 10 février 2009 relatif à la rémunération de certains services rendus par l'Etat consistant en une valorisation de son patrimoine immatériel.
- Décret n° 2010-862 du 23 Juillet 2010 relatif aux groupements de coopération sanitaire.
- Décret n° 2016-211 du 26 février 2016 relatif aux filiales et aux prises de participation des centres hospitaliers universitaires, JORF n°0050 du 28 février 2016 texte n°4.
- Décret n° 2018-687 du 1er août 2018 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiées par la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles.

Ordonnances

- Ordonnance n° 96-50 du 24 janvier 1996 relative au remboursement de la dette sociale.

- Ordonnance n° 96-51 du 24 janvier 1996 relative aux mesures urgentes tendant au rétablissement de l'équilibre financier de la sécurité sociale.
- Ordonnance n° 96-345 du 24 avril 1996 relative à la maîtrise médicalisée des dépenses de soins.
- Ordonnance n° 96-346 du 24 avril 1996 portant réforme de l'hospitalisation publique et privée.
- Ordonnance n° 2005-650 du 6 juin 2005 relative à la liberté d'accès aux documents administratifs et à la réutilisation des informations publiques.
- Ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives.
- Ordonnance n° 2015-1341 du 23 octobre 2015 relative aux dispositions législatives du code des relations entre le public et l'administration.
- Ordonnance n° 2015-1341 du 23 octobre 2015 relative aux dispositions législatives du Code des relations entre le public et l'administration.
- Ordonnance n° 2016-307 du 17 mars 2016 portant codification des dispositions relatives à la réutilisation des informations publiques dans le code des relations entre le public et l'administration.
- Ordonnance n° 2018-1125 du 12 décembre 2018 prise en application de l'article 32 de la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles et portant modification de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et diverses dispositions concernant la protection des données personnelles.

Circulaires

- Circulaire du 14 février 1994 relative à la diffusion des données publiques.

Textes européens

- Traité sur le fonctionnement de l'Union européenne (TFUE), anciennement traité instituant la Communauté européenne (TCE) établi par le traité de Rome de 1957.
- Traité sur l'Union européenne (TUE) établi par les accords de Maastricht en 1992.
- Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016.

Autres

- Enregistrements vidéo du Colloque « Le droit administratif au défi du numérique », Colloque annuel de l'Association Française pour la recherche en Droit Administratif, tenu du jeudi 14 juin 2018 au vendredi 15 juin 2018 à l'Université de Bordeaux, disponible sur https://www.canal-u.tv/ :

https://www.canal-u.tv/producteurs/universite_de_bordeaux/colloques/le_droit_administratif_au_defi_du_numerique

TABLE DES MATIERES