Université de Rennes 1

Faculté de Droit et de Science Politique

Ecole des Hautes Etudes en Santé Publique

Master 2 Droit de la santé

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

Le tryptique du traitement des données de santé : enjeux de santé publique, éthiques et Protection par le Droit

Mathilde Grente

Vendredi 9 septembre 2022

Sous la direction de Maître Florence Eon-Jaguin, avocate associée au Cabinet Withlaw et chargée d'enseignements à la Faculté de Droit de Rennes 1

Membres du jury :

Madame Florence Eon-Jaguin, Directrice de mémoire, avocate associée au Cabinet Withlaw et chargée d'enseignements à la Faculté de Droit de Rennes I

Madame Frédérique Michéa, Maître de conférences, Co-directrice du Master 2 "Droit de l'Union européenne" et co-responsable de la mention "Droit européen" à la Faculté de Droit de Rennes I

La Faculté de Droit de Rennes 1 et l'Ecole des Hautes Etudes en Santé Publique n'entendent donner aucune approbation, ni improbation aux propos émis dans ce mémoire, devant être considérés comme propres à leur auteur.

Remerciements

Je tiens à adresser mes sincères remerciements à Madame Florence Eon-Jaguin pour son aide, ses conseils et son œil expert dans la rédaction de ce mémoire.

Je remercie Madame Marie-Laure Moquet-Anger, directrice du Master 2 Droit de la santé, pour le partage de son savoir et de son expérience, ainsi que l'ensemble des intervenants du Master.

Je souhaite aussi adresser mes remerciements à Messieurs Nicolas Milleville et Olivier Bonaventur, mes tuteurs de stage qui ont permis d'alimenter ce travail et d'aiguiller mes ambitions professionnelles. Une pensée particulière pour les représentants des usagers de la Polyclinique St Laurent de Rennes, dont l'aide m'a été précieuse.

Une pensée également pour ma famille qui a bien évidemment contribué à la réussite de mes études et à mon épanouissement personnel et professionnel.

Un grand merci à mes amis pour leur soutien et leur patience durant ces cinq années de droit.

Enfin, je remercie affectueusement Jean-Malo Lebreton pour sa présence, sa bienveillance et ses précieux encouragements.

Sommaire

Liste des abréviations

AIPD : Analyse d'impact sur la protection des données

AFDS : Association française de droit de la santé

ANS : Agence du numérique en santé

ARS : Agence régionale de santé

ASIP-Santé : Agence des systèmes d'information partagés de santé

CépiDC : Centre d'épidémiologie sur les causes médicales de décès

CCNE : Comité consultatif national d'éthique

CE : Conseil d'Etat

ConvEDH : Convention européenne des droits de l'homme

CEDH : Cour européenne des droits de l'homme

CEPD : Comité Européen de la Protection des Données

CH : Centre hospitalier

CHU : Centre hospitalier universitaire

CSP : Code de la Santé publique

CSS : Code de la Sécurité sociale

CNAM : Caisse Nationale d'Assurance Maladie

CNIL : Commission nationale de l'informatique et des libertés

CNOM : Conseil national de l'Ordre des médecins

CPP : Comité de Protection des Personnes

DGOS : Direction générale de l'offre de soins

DMP : Dossier médical personnel devenu Dossier médical partagé depuis la LOI n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé

DP : Dossier pharmaceutique

DPD : Délégué à la Protection des données

DNS : Délégation du numérique en santé

DSI : Directeur/ Direction des systèmes d'information

EHPAD : Etablissement d'hébergement pour personnes âgées dépendantes

ENS : Espace numérique de santé

ES : Etablissement de santé

G29 : Groupe de travail de l'article 29 de la directive n° 95/46/CE sur la protection des données

GAFAM: Google, Apple, Facebook, Amazon, Microsoft

GCS : Groupement de coopération sanitaire

GHT : Groupement hospitalier de territoire

HAS : Haute Autorité de Santé

HDH : Health Data Hub

HDS : Hébergeur/hébergement de données de santé

HSE : Health Service Executive

HSTV : Hospitalité Saint Thomas de Villeneuve

INDS : Institut National des Données de Santé

INSERM : Institut national de la santé et de la recherche médicale

LIL : Loi dite Informatiques et Libertés

Loi HPST : Loi n° 2009-879 du 21 juillet 2009 portant réforme de l'hôpital et relative aux patients, à la santé et aux territoires

Loi MNSS : Loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé

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

MR : Méthodologie de référence

MSS : Messagerie sécurisée de santé

ONDAM : Objectif national des dépenses de l'assurance maladie

PCS : Pro santé connect

PMSI : Programme de Médicalisation des Systèmes d'Information

PGSSI-S : Politique Générale de Sécurité des Systèmes d'Information de Santé

RGPD : Règlement RGPD Règlement relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (Règlement général sur la protection des données)

RIPH : Recherches Impliquant la Personne Humaine

SI-DEP : Système d'information national de suivi et de dépistage

SNIIRAM : Système national d'information inter-régimes de l'Assurance maladie

SSI : Sécurité des systèmes d'information

SNDS : Système National des Données de Santé

TFUE : Traité sur le fonctionnement de l'Union européenne

Introduction

« *La donnée de santé est un objet de droit. Elle est même au centre d'un réseau de règles juridiques en tant qu'elle est une donnée et en tant qu'elle concerne la santé. Mais elle n'est pas un objet "inerte" : elle rétro-agit, en quelque sorte, sur le corps de règles dans lequel elle s'insère. Il s'agit, ici, surtout de l'information sur la santé du patient, donc des droits et obligations de ce dernier, et de tous ceux pour lesquels cette information présente un intérêt. Selon un processus classique d'évolution du droit, la donnée de santé obéit à la fois à des règles propres qu'elle suscite et à des règles antérieures dont elle affecte les modalités d'application.* » [1] Telle est l'analyse de Didier Truchet, ancien Président de l'Association Française de Droit de la santé, soulevée lors d'un colloque sur le Droit des données de santé organisé le 25 mars 2004. La donnée de santé interroge les juristes, car elle est l'essence même de l'intimité des personnes, et est dans le même temps une information possiblement partagée et échangée entre plusieurs acteurs. Ainsi, l'essor de l'utilisation du numérique dans le monde de la santé amorce une inquiétude : comment concilier la protection de la vie privée des personnes dont sont recueillies et exploitées les données de santé avec la nécessité de partager ces données, dans des objectifs de santé publique, de prise en charge sanitaire et de recherche médicale ?

Dans le cadre de mon stage au sein de la Polyclinique Saint-Laurent, établissement du groupe Hospitalité Saint-Thomas de Villeneuve, j'ai pris conscience de la méconnaissance des patients quant à l'usage qui était fait de leurs données de santé. Après avoir été sensibilisée sur la question par Monsieur Milleville, mon tuteur et le Délégué à la Protection des Données (DPD) du groupe HSTV, j'ai pris attache avec deux représentants des usagers de la Polyclinique Saint-Laurent. Ensemble, nous avons créé un questionnaire[2] sur le consentement des patients au traitement de leurs données de santé. Je souhaitais leur laisser la parole sur un sujet les concernant directement. Après accord de la Direction, la Responsable qualité-risques de la Polyclinique nous a orientés vers six services susceptibles d'avoir des patients en état de répondre à mes questions : la pneumologie, l'USSR, la cardiologie, la chirurgie, la psychiatrie et l'addictologie. Douze questionnaires à douze patients différents ont été distribués, en compagnie des représentants des usagers. A chaque personne, une explication succincte de l'objet de l'étude était fournie ainsi que la signification des termes « donnée de santé »,

[1] Propos retranscrits dans le numéro spécial « Droit des données de santé » RGDM, 2004, page 10
[2] Annexe 1 : Questionnaire

« RGPD », « traitement informatique ». Les retours[3] des patients sur ce questionnaire ont nourri ma réflexion, m'ont permis d'élaborer les prémices de ce que je souhaitais écrire dans ce mémoire. Il m'est donc apparu évident de traiter l'enjeu majeur que représente le traitement informatisé des données de santé. Ce traitement est pourtant prohibé par les textes, mais ce principe est assorti d'exceptions à mettre en lumière. Il s'agit également d'apporter des réponses liées aux enjeux éthiques du recueil des données de santé et aux problématiques de leur encadrement par le Droit.

Le sujet est fort d'une transversalité entre Droit de la santé, Droit du numérique et Droit européen. A ce titre, il nécessite à la définition de plusieurs termes :

Traitement. Selon l'article 4 du Règlement Général sur le Protection des Données[4] (RGPD), un « traitement de données personnelles » est une opération, ou ensemble d'opérations, portant sur des données personnelles, quel que soit le procédé utilisé (collecte, enregistrement, organisation, conservation, adaptation, modification, extraction, consultation, utilisation, communication par transmission diffusion ou toute autre forme de mise à disposition, rapprochement). Un traitement de données doit avoir un objectif, une finalité. A chaque traitement de données doit être assigné un but, qui doit bien évidemment être légal et légitime au regard de l'activité en cause. [5] Cette définition complexe justifie que l'on entende la collecte, l'utilisation des données de santé au sens large de « traitement ».

Le traitement des données de santé est à différencier du traitement au sens médical du terme, qui est selon le Larousse médical, « *l'ensemble des méthodes employées pour lutter contre une maladie et la guérir* ».

Le traitement des données de santé répond aujourd'hui à l'informatisation des processus de soins, des dossiers médicaux, des protocoles, des prescriptions et également aux nouvelles pratiques professionnelles portées par la numérisation du monde de la santé, comme l'échange et le partage via la Messagerie Sécurisée de Santé (MSS). Il concerne aussi bien les professionnels des secteurs sanitaire, social et médico-social, les organismes de santé et de sécurité sociale, les acteurs institutionnels tels que les ministères, les agences sanitaires, les agences régionales de santé et les industriels de la santé.

[3] Annexe 2 : Retour des patients de la polyclinique Saint Laurent sur le traitement de leurs données de santé
[4] 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
[5] https://www.cnil.fr/fr/rgpd-de-quoi-parle-t-on

Au premier plan, le traitement des données de santé regarde évidemment les usagers du système de santé, car ce sont bien leurs informations intimes qui sont exploitées.

Données à caractère personnel. Au sens de de l'article 4.1 du RGPD, toute information se rapportant à une personne physique identifiée ou identifiable. Est réputée être une «personne physique identifiable» une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale.

Données de santé. La donnée se distingue de l'information, en ce sens qu'elle comporte une plus-value technologique, destinée à son traitement. La donnée de santé est avant tout une donnée à caractère personnel, définie ci-dessus. En 1988, de manière très large, Isabelle Vacarie définissait les données de santé comme « *les données concernant l'état de santé de la personne, ses problèmes de santé. Ces données révèlent ses affections ou ses handicaps.* » [6] Une définition juridique a été donnée par le RGPD, texte de référence en matière de protection des données à caractère personnel. Adopté le 27 avril 2016 par le Parlement Européen et le Conseil de l'Union Européenne, il est entré en application en France le 25 mai 2018. Son article 4-15 dispose dès lors que les données concernant la santé sont *« les données à caractère personnel relatives à la santé physique ou mentale d'une personne physique, y compris la prestation de services de soins de santé, qui révèlent des informations sur l'état de santé de cette personne ».* Cela peut être des antécédents médicaux, des traitements médicamenteux, des résultats d'examens.

L'article 9 du RGPD emploie le terme de « *catégories particulières de données* » pour parler des données de santé. On retrouve dans cette catégorie, 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 de cette personne physique et qui résultent, notamment, d'une analyse d'un échantillon biologique de la personne physique en question »*[7] et les données biométriques, *« résultant d'un traitement technique spécifique, relatives aux caractéristiques physiques, physiologiques ou*

[6] I. Vacarie, rapport au Commissariat général du plan sur Le Traitement informatique des données de santé – Questions juridiques et éthiques
[7] Article 4-13 du RGPD

comportementales d'une personne physique, qui permettent ou confirment son identification unique, telles que des images faciales ou des données dactyloscopiques »[8]

Trois catégories de données de santé sont à distinguer, collectées à l'occasion d'une prise en charge sanitaire, d'une prestation de soins ou de la participation à une recherche médicale :

- Les données de santé par nature, informant directement sur la santé de la personne concernée comme des résultats d'examens ou des antécédents médicaux ;
- Les données de santé, qui du fait de leur croisement avec d'autres données deviennent des données de santé, tel que l'indice de masse corporelle croisant le poids et la taille ;
- Les données de santé par destination, qui deviennent des données de santé du fait de l'utilisation qui en est faite au plan médical. Pour cette dernière catégorie, il convient de donner l'exemple de la collecte de données sur l'origine ethnique aux fins de réaliser une meilleure évaluation du risque pour certaines pathologies, selon les lieux de naissance, les appartenances ethniques etc.

Il est aujourd'hui observé, un traitement des données de santé massif, qui interroge leur protection. La logique des Big Data[9] incite à une collecte de données toujours plus importante. A cet égard, les données personnelles des patients constituent une source d'information dont l'exploitation par les hôpitaux, les chercheurs et les organismes de santé est nécessaire. Elles représentent aussi une mine d'or pour certaines entreprises, comme les GAFAM, géants du Web américain. Cela soulève de nouveaux enjeux juridiques et éthiques, selon le docteur Pierre Simon, fondateur de la Société Française de télémédecine, qui alerte sur la surveillance par les Etats de l'état de santé de leurs populations. [10]

Parmi les actions menées pour accompagner l'essor du numérique en santé, la Politique Générale de Sécurité des Systèmes d'Information de Santé (PGSSI-S), corpus de référentiels et de documents édictés par le Ministère des solidarités et de la santé fixent des exigences en matière de sécurisation des données de santé et sensibilise les établissements et professionnels de santé aux risques liés à la manipulation des données de santé. Les patients s'en voient rassurés, mais seulement 52% d'entre eux déclarent avoir confiance dans les autorités de santé quant aux risques liés au données de santé selon les chiffres de l'Agence des systèmes

[8] Article 4-14 du RGPD
[9] C'est-à-dire les données massives.
[10] « Les big data au service de la télésurveillance médicale des patients atteints de maladies chroniques », Journal du Droit de la Santé et de l'Assurance - Maladie (JDSAM), vol. 20, no. 3, 2018, pp. 7-11.

d'information partagés de santé (ASIP-santé), nouvellement Agence du Numérique en Santé (ANS).

En outre, les données de santé, lesquelles sont cotées sur le marché noir de la donnée, sont sources de risques importants : vol de données, destruction ou modification malintentionnée, piratage etc. Autant de risques qui exposent les données de santé à des fuites et les patients à de mauvaises prises en charge. Deux exemples récents nous sont donnés. Le 21 aout 2022, l'hôpital Sud Francilien, à Corbeil-Essonnes était victime d'une attaque informatique, rendant inaccessible les logiciels métiers, les systèmes d'imagerie médicale et le logiciel d'admission du centre hospitalier. Cette situation de crise a nécessité le déclenchement d'un plan blanc[11] par le directeur de l'établissement et la réorientation des patients vers d'autres structures en Ile-de-France. Le corps médical a dû passer en mode dégradé, c'est-à-dire se passer de l'outil informatique pour reprendre les procédures écrites sur papier. La rançon exigée est de 10 millions d'euros, et à l'heure où ces lignes sont écrites, la situation n'est pas réglée, en dépit de la mobilisation des équipes informatiques du CH et des forces de l'ordre spécialisées dans la lutte contre la cybercriminalité.

Aussi, le 17 mars 2022, l'Assurance maladie annonçait une fuite de données administratives de 510 000 assurés sociaux. Fruit d'une cyberattaque, cette fuite concerne des données personnelles telles que les noms et prénoms mais plus délicat encore, des données relatives aux droits : déclaration d'un médecin traitant, attribution de la complémentaire santé solidaire ou de l'aide médicale d'État, éventuelle prise en charge à 100 % etc. Selon l'Assurance Maladie, « *des personnes non autorisées ont réussi à se connecter à des comptes amelipro, réservés aux professionnels de santé. Il ressort des premières analyses que les attaquants ont pu se connecter à des comptes dont les adresses e-mail avaient été compromises (19 comptes de professionnels de santé ont été identifiés).* » De quoi avertir la CNIL et déposer une plainte au pénal.[12] Le problème n'est pas national, mais bien européen et international. Pour preuve, dans la nuit du 14 mai 2020, le Health Service Executive (HSE), l'organisation publique de la santé en Irlande a subi une attaque informatique de grande ampleur. Plus de 40 établissements de santé irlandais, dont une majorité d'hôpitaux, ont été impactés annonçait l'Agence du Numérique en santé dans un article du 21 septembre 2021.

[11] Créé par la loi n° 2004-806 du 9 août 2004 relative à la politique de santé publique : plan spécifique d'urgence sanitaire pour planifier la mise en œuvre rapide et rationnelle des moyens indispensables en cas de crise (afflux de victimes, attaques informatiques, terrorisme etc.)

[12] Communiqué de presse "Connexion de personnes non autorisées à des comptes amelipro » 17 mars 2022 https://assurance-maladie.ameli.fr/sites/default/files/2022-03-17-Infopresse-Connexions-non-autorisees-comptes-amelipro.pdf

Pour comprendre ce phénomène et saisir l'enjeu de la sécurisation des données de santé, Orange Healthcare a publié des chiffres clés : un dossier médical sur le Darkweb se revend à quinze euros. C'est par comparaison, la valeur des accès à trente mille comptes e-mail. En 2017, 27 % des 2,7 millions de fuites de données concernaient des données de santé. C'est bien plus que les données de gouvernements (11%)[13]

Or, le constat dressé est celui de la numérisation de la santé. Selon la Haute Autorité de Santé (HAS), *« la puissance publique s'est donnée pour ambition d'accélérer le virage numérique du système de santé* »[14]. Quatre thématiques essentielles et complémentaires ont alors émergé, telles que l'impact du numérique sur l'usager du système de santé et d'accompagnement social, qui doit permettre son engagement dans son propre parcours de santé ou de vie ; les capacités du numérique pour améliorer la qualité des soins et des accompagnements et le travail des professionnels dont c'est le métier ; l'exigence de qualité et d'efficacité des technologies numériques, qui doit être assurée par leur évaluation pour gagner la confiance des usagers, des professionnels et des structures et établissements de soins et d'accompagnement ; et enfin, le sens général que la puissance publique devrait donner au virage numérique en santé et dans le social. Ces quatre points sont assortis de propositions pour faire du numérique « un levier de l'amélioration de la qualité, de l'efficacité et de l'efficience de notre système de santé et d'accompagnement social. »[15]

Le Gouvernement, suite au Ségur de la santé, s'est donné une feuille de route ambitieuse pour accélérer le virage du numérique en santé : deux milliards d'euros, dont 600 millions pour le médico-social. L'Institut Montaigne, plateforme de réflexion consacrée aux politiques publiques argue même que *« le déploiement de la e-santé associé à un recueil systématique des données de santé fait partie des bases indispensables sur lesquelles doit reposer notre système de soins. Cette digitalisation est essentielle pour répondre aux nombreux défis auxquels le système fait face : l'explosion des maladies chroniques, le vieillissement de la population, l'évolution du nombre de soignants sur le territoire, la soutenabilité économique du système de santé et les nouveaux défis sanitaires et sociaux. (…) »* Preuve en est l'essor de la télémédecine, pratique médicale effectuée à distance par un médecin en mobilisant les technologies de l'information et de la communication.

[13] https://healthcare.orange.com/fr/dossiers/securite-des-donnees-de-sante/
[14] HAS. Rapport d'analyse prospective 2019, « Numérique : quelle (R)évolution ? »
[15] Rapport d'analyse prospective : "Numérique : quelle (R)évolution ? HAS, 2019, page 16

La loi du 21 juillet 2009[16] la définit et la règlemente, complétée par le décret du 19 octobre 2010[17] venant préciser les cinq actes médicaux réalisables en télémédecine : la téléconsultation, la téléexpertise, la télésurveillance médicale, la téléassistance et la régulation. Plébiscitée durant la crise du Covid 19, cette nouvelle pratique est désormais inscrite dans le droit commun. L'article 78 de la loi HPST a modifié le code de la santé publique afin d'y intégrer la définition de la télémédecine à l'article L. 6316-1. De manière dérogatoire, ces actes de téléconsultation sont pris en charge à 100% par l'Assurance Maladie jusqu'au 31 juillet 2022. D'ordinaire, dans le respect d'un parcours de soins coordonnés, la téléconsultation est remboursée à hauteur de 70% mais prise en charge à 100% dans le cas d'une affection de longue durée, d'une grossesse ou de patients disposant de la Complémentaire santé solidaire.

Ces ambitions affirmées de numériser la santé, quoi qu'il en coûte, interrogent sur la protection des droits fondamentaux. En effet, le droit au respect de la vie privée et familiale, consacré à l'article 8 de la Convention Européenne des Droits de l'Homme (ConvEDH) et à l'article 7 de la Charte des droits fondamentaux de l'Union Européenne, est l'exemple typique des risques dont l'ampleur a été accrue par le traitement massif des données de santé. Face à ces enjeux de protection, un cadre juridique encadrant le traitement des données personnelles de santé était nécessaire. De longue date, et parce que le RGDP n'a fait que compléter la législation française, les pouvoirs publics avaient pris conscience qu'un traitement sécurisé des données de santé passait par une réglementation stricte. C'est la genèse de la loi du 6 janvier 1978[18], dite Loi Informatiques et Libertés (LIL). Pour compléter ce cadre, il importe également de tenir compte des dispositions introduites par le décret 2019-536 du 29 mai 2019[19] venant la compléter. D'autres textes de notre corpus juridique encadrent l'utilisation des données de santé : le Code de santé publique (CSP) et le Code de sécurité sociale (CSS).

Par principe, les données de santé, en raison de leur extrême sensibilité, ne peuvent pas être collectées et traitées. Mais ce principe est assorti d'exceptions, concourant au bon fonctionnement du système de santé. En effet, la loi du 6 janvier 1978 entérine en son article 6, le principe, figurant également à l'article 9 du RGPD, de l'interdiction de traitement des

[16] Loi n° 2009-879 du 21 juillet 2009 portant réforme de l'hôpital et relative aux patients, à la santé et aux territoires, dite HPST
[17] Décret n° 2010-1229 du 19 octobre 2010 relatif à la télémédecine

[18] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés
[19] Décret n° 2019-536 du 29 mai 2019 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés

données de santé. *« Il est interdit de traiter des données à caractère personnel qui révèlent la prétendue origine raciale ou l'origine ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale d'une personne physique ou de traiter des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique».* Cependant, de nombreuses exceptions ont été posées dans la loi, confirmées par le récent RGPD, noyant ainsi le principe d'interdiction et confirmant ainsi que le Droit n'est pas le Droit sans la multitude d'exceptions au principe originel. Ce dispositif juridique mérite une analyse approfondie.

De cet état de droit, posé par l'interdiction de principe de traiter les données, accompagnée d'exceptions multiples concourant à la prise en charge sanitaire, à la gestion de la santé publique, mais encore à l'urgence, la recherche médicale… il est nécessaire d'étudier ce principe et d'examiner ses modalités pratiques de mise en œuvre par les établissements, les professionnels et les organismes de santé. Premièrement, dans quelle mesure le traitement des données de santé permet-il de servir les enjeux de santé publique ?

Secondairement, le consentement constitue une exception majeure au principe d'interdiction du traitement des données de santé. Comment s'articule l'interdiction de principe de traitement des données de santé avec cette exception ? Faisant partie d'une liste de dix exceptions, et contrairement à ce qui a pu être écrit et commenté à la suite de l'entrée en vigueur du RGPD en mai 2018, il s'avère en pratique qu'il n'est pas la base juridique la plus fréquemment utilisée pour justifier le traitement des données personnelles de santé. Aussi, il est impératif de s'intéresser à la place laissée au consentement du patient dans le traitement des données personnelles de santé.

Enfin, les autorités régulatrices et juridictionnelles exercent- elles un contrôle suffisant pour protéger le traitement des données de santé, et quelle interprétation font-elles de l'interdiction de principe de traiter les données de santé ? Les contours de cette question nous obligeront à effectuer une balance entre l'attachement sociétal au respect de la vie privée et les enjeux que représentant le traitement des données de santé pour la santé publique.

L'analyse juridique sera complétée par l'expérience de professionnels rencontrés dans le cadre de stages à la Clinique Saint-Laurent et au Centre Mutualiste de Kerpape, confrontés, d'une part aux difficultés d'appréhension du droit des données de santé, et d'autre part aux enjeux éthiques. L'approche éthique sera également appuyée sur un entretien mené avec la

Délégation ministérielle au Numérique en Santé (DNS), rattachée au Ministère des solidarités et de la santé et assurant la tutelle de l'Agence du Numérique en Santé.

Si le traitement des données de santé comporte un fort enjeu de santé publique au regard des progrès médicaux et scientifiques qu'il permet au bénéfice des citoyens (**Partie I**), il n'en reste pas moins qu'il doit être effectué dans le respect des règles relatives à la protection des données personnelles afin de veiller au respect de la vie privée des patients. Un équilibre est donc à trouver. Les règles en vigueur formalisent cet équilibre, actuellement incarné au plan juridique par le dispositif sus décrit.

Ce traitement est tempéré du principe d'interdiction de collecte assortie d'exceptions énumérées de façon limitative. L'étude de ces exceptions nous conduira à envisager les enjeux éthiques d'un tel traitement, et les réponses des autorités régulatrices et juridictionnelles face aux difficultés posées par l'interprétation du principe (**Partie II**).

Partie I : Le traitement des données de santé, un enjeu de santé publique

Le traitement des données de santé des patients pris en charge en établissement de santé, en structures de ville ou au cours d'une visite en officine pharmaceutique, est une condition à la prise en charge et à la réalisation des soins et des traitements. Par exemple, aussi bien pour le secteur hospitalier que pour la médecine de ville, les données de santé permettent un suivi, une connaissance de l'état de santé du patient. Les données servent également et concomitamment les enjeux de santé publique, afin d'effectuer une surveillance épidémiologique et une veille sanitaire à l'appui d'acteurs tels que Santé Publique France et les ARS. Le recueil de données médicales est ainsi inhérent aux fins de la médecine, de l'administration du système de santé et d'assurance-maladie et de la santé publique. Les traitements de données de santé ne peuvent être mis en œuvre qu'en considération des finalités qu'ils présentent, dont notamment la garantie de normes élevées de qualité et de sécurité concernant les soins de santé et des médicaments ou des dispositifs médicaux.

Si ces utilisations des données de santé sont louables, leur usage peut être source de dérives, notamment pour les libertés publiques, justifiant un principe général d'interdiction du traitement des données de santé (Chapitre 1), relativisé par les exceptions légalement consacrées dont celle relative au consentement de la personne concernée (Chapitre 2).

Chapitre I : Le principe d'interdiction du traitement des données de santé entériné mais à relativiser dans sa mise en œuvre

Le règlement européen à l'article 9 et la loi Informatique et Libertés à l'article 6 posent un principe d'interdiction des traitements de données de santé (Section 1). Cette interdiction n'est qu'un principe, qui conduit nécessairement à la prudence en matière d'utilisation des données de santé. Cette interdiction est toutefois à relativiser, en particulier au regard de l'usage autorisé au profit des acteurs institutionnels, dans l'intérêt du système de santé (Section 2).

Section I : Une confirmation du principe d'interdiction par le Règlement Général sur la Protection des Données Personnelles, antérieurement admis par la loi Informatiques et Libertés

"L'informatique doit être au service de chaque citoyen. [...]. Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques" [20] Telle était l'esprit de la loi de 1978, venue encadrer le traitement des données à caractère personnel en France et souhaitant éviter le fichage des personnes. Les données de santé, considérées comme sensibles, furent l'objet d'un article 8 disposant qu' « *Il est interdit de traiter des données à caractère personnel qui révèlent (…), des données concernant la santé (…)* ». Disposant ainsi d'un cadre juridique contraignant (§1) sous-tendu par l'interdiction de les traiter, il n'en demeure pas moins que les données de santé sont exploitées par les acteurs institutionnels dans l'intérêt des patients et du système de santé (§2) et qu'ils disposent à ce titre, d'un « laissez-passer » juridique pour l'exercice de leurs missions.

§1 : Le traitement des données de santé, un cadre juridique contraignant

« *L'usage d'internet et sa portée étant universels, l'enjeu est celui du niveau et de l'aire territoriale de la protection et des garanties offertes par le droit applicable. L'Union européenne et ses membres se sont inscrits dans la perspective d'une protection élevée qui, sans conduire à une extraterritorialité agressive de ses lois, doit permettre de les appliquer de manière très large à tous ses résidents et de sauvegarder et renforcer ainsi les garanties de chacun.* »[21] Cette citation de Jean Marc-Sauvé ramène à l'essence de la rédaction du RGPD, suite à l'échec de la directive de 1995[22]. La lettre du règlement est celle d'une harmonisation des règles européennes (*A*), afin de permettre une protection uniforme et renforcée des droits des citoyens face à leurs données personnelles de santé (*B*). Ceci est la réponse nécessaire au défi que pose la numérisation de la santé face au respect de la dignité et de l'auto-détermination de l'être humain.

[20] Article 1er, Loi n° 78-17 du 6 janvier 1978 dite " Loi Informatique et Libertés »
[21] La protection des droits fondamentaux à l'ère du numérique Fondation Varenne, Mardi 12 décembre 2017 Intervention de Jean-Marc Sauvé, vice-président du Conseil d'État
[22] Directive 95/46/CE du Parlement européen et du Conseil, du 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

A) L'harmonisation européenne des règles relatives au traitement des données de santé

Deux temps ont marqué l'évolution et la consécration du cadre juridique des données de santé. Un premier a été l'arrimage de la protection des données de santé à celle de la vie privée. En 1981, est adoptée par le Conseil de l'Europe, la Convention STE n° 108 du Conseil de l'Europe sur la protection des personnes à l'égard du traitement automatisé des données à caractère personnel. Selon Sophie Gambardella, « *La Convention est innovante pour l'époque dans la mesure où si elle s'applique à traiter de la protection des données à caractère personnel à travers le droit au respect de la vie privée, elle envisage, dans le même temps, l'équilibre fragile mais nécessaire entre liberté d'expression et protection des données* »[23] Ce texte, plus méconnu que la LIL ou le RGPD est pourtant l'un des premiers à garantir aux membres des Etats l'ayant signé, le respect de leurs droits et libertés fondamentaux dans le cadre du traitement informatique des données personnelles. La Convention s'inscrit dans la volonté du Conseil de l'Europe *« d'étendre la protection des droits et des libertés fondamentales de chacun, notamment le droit au respect de la vie privée, eu égard à l'intensification de la circulation à travers les frontières des données à caractère personnel faisant l'objet de traitements automatisé ».*[24]

Dans un second temps, la protection des données de santé a connu une complexité technique du fait d'un amoncèlement de textes juridiques, causant perplexité et incohérence aux établissements, professionnels, et organismes chargés de traiter des données de santé. Le principe, inscrit dans le marbre de la loi de 1978 est celui de l'interdiction. Sur le pan du droit européen, la directive 95/46/CE du Parlement européen et du Conseil confirme cela et fera l'objet d'une transposition dans le droit national par la loi du 6 aout 2004[25], modifiant par la même occasion la loi de 1978.

Face à la nécessité d'harmoniser les règles relatives à la protection des données à caractère personnel, dont les données de santé, le RGPD est adopté dans une optique de simplification et d'intelligibilité du droit. Il renforce les droits des personnes, principales concernées par le traitement de leurs données de santé et en crée de nouveaux. Il impose le respect de grands

[23] « Une lecture de la jurisprudence de la Cour européenne des droits de l'Homme relative aux données de santé», RDSS, 2016, n°2, pp. 271 et s.
[24] Préambule de la Convention n°108
[25] Loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel

principes en son article 5 tels que la licéité, la transparence et la loyauté du traitement des données à caractère personnel. Il s'agit de donner confiance aux citoyens.

Pour autant, le cadre juridique posé par la loi de 1978 ne disparaît pas, il évolue en impactant nettement le secteur de la santé car le RGPD définit pour la première fois la donnée de santé et confirme le principe de l'interdiction de son traitement. Dans la droite ligne de la législation de 1978, les exceptions à ce principe sont confirmées.

Comme le rappelle l'ANS, « *Le RGPD porte sur toutes les données personnelles issues des activités de l'établissement de santé, et pas uniquement sur les données de santé générées par la prise en charge des personnes. »*[26] Ces activités sont générées par l'informatisation des processus de soins, les moyens d'échange et de partage entre professionnels de santé, les logiciels d'aide à la prescription, mais aussi les activités administratives à l'origine de données médico-administratives (prestations sociales, handicap, profession…)

Un des effets juridiques notables du RGPD est son application extra territoriale. Le règlement européen et la directive du 27 avril 2016[27] confirment l'affaiblissement du critère géographique ou territorial, puisqu'ils vont s'appliquer même lorsque les traitements en cause sont effectués hors de l'Union européenne par une société elle-même établie hors de l'Union dès lors que les personnes concernées par ce traitement ressortent de l'UE. Les traitements de données personnelles extra-européens des résidents européens sont ainsi régis par le droit de l'UE. Ces nouvelles règles constituent un gain de confiance pour les citoyens car l'Union européenne « *dispose d'un standard élevé de protection des personnes physiques à l'égard des traitements de données, qui est regardé comme la norme ayant vocation à servir de référence dans le monde » selon le Conseil d'État*[28]

Le RGPD a instauré une unification du droit des données personnelles sur le plan juridique. Dans les faits, la numérisation du monde de la santé doit passer par une sensibilisation car l'informatisation conduit à repenser les modes de traitement des données de santé. Ainsi, l'esprit du règlement est celui d'une responsabilisation renforcée des acteurs *(B*).

[26] RGPD : Présentation générale et impacts en établissement de santé, p.5 Mai 2018 – ANS et CNIL
[27] Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016
[28] La protection des droits fondamentaux à l'ère du numérique- Fondation Varenne, Mardi 12 décembre 2017 Intervention de Jean-Marc Sauvé, vice-président du Conseil d'État

B) L'esprit du RGPD : responsabiliser les acteurs, dont les responsables de traitement de données de santé

Bien que sensibles à la question avant l'arrivée du RGPD, les acteurs de santé ont connu une responsabilisation croissante du traitement qu'ils faisaient des données de santé. Venant s'ajouter à leur mission principale de soins, les établissements de santé ont dû prendre la mesure de l'introduction par le règlement européen de 99 articles, qui impose désormais un haut niveau de protection de la vie privée lorsque des traitements de données de santé sont générés, à l'appui de nouveaux principes :

- Le « *privacy by design* »[29] et le « *privacy by default* »[30] . Ces deux systèmes permettent, dès la conception d'un traitement de données, de garantir aux personnes un haut niveau de protection de leurs données. Plus précisément, le *privacy by default* permet de garantir que, par défaut, seules les données strictement nécessaires au regard de la finalité ne seront traitées.
- Le principe d' « *accoutability* » qui désigne l'obligation pour les établissements de santé de mettre en œuvre des mécanismes et des procédures internes permettant de démontrer le respect des règles relatives à la protection des données.

Au travers de ces principes, est consacrée une logique de responsabilisation des responsables de traitement, et donc des établissements de santé. Le RGPD a changé le paradigme en matière de traitement des données personnelles. Auparavant, une procédure a priori en cas de traitement des données prenait la forme d'autorisation. Exceptionnellement, une procédure d'autorisation en amont peut exister mais une vérification en aval par la CNIL et les juridictions est plus largement prévue. Cela démontre le passage d'un contrôle a priori à un contrôle a posteriori. C'est aux acteurs de se mettre en conformité avec la règle.

L'on peut aisément imaginer que cela a questionné les pratiques lors de l'entrée en vigueur du RGPD, mais ce dernier reste pourtant évasif quant aux « mécanismes et procédures internes » à mettre en œuvre.

En pratique, ce principe est déployé au travers de l'obligation a minima de tenir un registre des traitements[31] de données personnelles, afin d'assurer leur traçabilité et d'en justifier l'importance. C'est également l'occasion d'identifier et anticiper les risques de l'utilisation

[29] Cette notion a été développée par A.CAVOUKIAN, préposée à la protection des données de l'état d'Ontario au Canada.
[30] Article 25 du RGPD
[31] Article 30 RGPD

des données. Cette obligation est assurée par le Délégué à la Protection des Données (DPD), dont les établissements de santé doivent désormais se doter. Son rôle ne se substitue pas au responsable de traitement, souvent le directeur d'établissement.

Le respect du principe d'accountability se lit également à travers l'obligation de réaliser des analyses d'impact relatives à la protection des données personnelles (AIPD), dans les cas prévus par le RGPD. La CNIL définit : « *L'AIPD est un outil qui permet de construire un traitement conforme au RGPD et respectueux de la vie privée, lorsqu'un traitement de données personnelles est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées.* » En somme, une analyse approfondie de l'utilisation des données est nécessaire lorsqu'elle concerne par exemple, des données sensibles de santé ou des données relatives à des personnes vulnérables. Dans le cadre de mon stage au sein d'HSTV, j'ai réalisé l'AIPD de l'application Mobil'eTY by Globule, messagerie instantanée de santé développée par le GCS e-santé Bretagne. Elle s'adresse à tout type d'utilisateur associé à la coordination de proximité : professionnels libéraux (médecin, infirmiers, kiné, pharmaciens, etc.), les établissements sanitaires, sociaux et médico-sociaux. Mobil'e TY associe un dossier structuré pour le patient / usager et un cahier de liaison mobile facilitant la communication et le partage entre professionnels, générant alors des traitements de données de santé, nécessitant une analyse des risques au regard de la protection imposée par le RGPD. L'AIPD se déroule en concertation avec le DPD et les professionnels utilisant l'application, et conduit, lorsque les principes fondamentaux de la protection des données sont respectés, à une validation du service numérique. De cette analyse d'impact, des risques pour la vie privée des personnes ont été identifiés, ainsi que des mauvaises pratiques de professionnels. Cela a été corrigé avant le lancement de l'application, qui permet aujourd'hui une coordination sans risque dans la prise en charge des patients.

En outre, il faut souligner que des règles sectorielles doivent être respectées par les professionnels de santé. A titre d'exemple, l'article L 1111-8-2 du CSP dispose que « *les établissements de santé et les organismes et services exerçant des activités de prévention, de diagnostic ou de soins signalent sans délai à l'agence régionale de santé les incidents graves de sécurité des systèmes d'information. Les incidents de sécurité jugés significatifs sont, en outre, transmis sans délai par l'agence régionale de santé aux autorités compétentes de l'État.* » Depuis le 18 novembre 2020, cette obligation a été étendue aux établissements médico-sociaux par ordonnance n° 2020-1407 du 18 novembre 2020 relative aux missions des ARS.

Le RGPD l'a encore renforcé en imposant de signaler auprès de la CNIL des incidents de sécurité impliquant des données personnelles ; ce qu'a récemment dû faire le GHT Grand Est suite à une cyberattaque massive sur ses réseaux le 19 avril 2022. Les données mises en vente sur le *dark-web*[32] font *« l'objet d'une demande de rançon ou de paiement à hauteur de 1,3 million de dollars pour [les] supprimer* », a développé Jérôme Goeminne, directeur du GHT en ajoutant qu'il ne serait pas donné suite à cette demande de rançon.[33] In fine, c'est 733 incidents de sécurité impactant des données de santé qui ont été déclarés en 2021. Ce nombre a presque doublé par rapport à 2020 (369), selon les chiffres de l'Observatoire des signalements d'incidents de sécurité des systèmes d'information pour le secteur santé.

En outre, les médecins, y compris ceux qui exercent en libéral, sont les premiers concernés par la responsabilité renforcée. L'usage qu'ils font des dossiers médicaux doit respecter les principes fondamentaux du droit des données à caractère personnel[34]. Un mésusage peut être sanctionné par la CNIL et l'Ordre des médecins si tel n'est pas le cas. Ainsi, sur la base du non-respect des prescriptions du RGPD et du CSP en matière de protection des données, deux médecins ont été condamnés par la formation restreinte de la CNIL à des amendes de 3000 et 6000 euros[35]. La Commission a retenu a retenu un manquement à l'obligation de sécurité des données[36], « *considérant qu'ils auraient notamment dû s'assurer que la configuration de leurs réseaux informatiques ne conduisait pas à rendre les données librement accessibles sur Internet et procéder au chiffrement systématique des données personnelles hébergées sur leurs serveurs. »* La formation restreinte a également retenu un manquement à l'obligation de notifier les violations de données à la CNIL, alors même que cela est de leur devoir. En effet, les deux médecins « *n'ont pas effectué ces notifications obligatoires auxquelles ils auraient dû procéder après avoir appris que les images médicales de leurs patients étaient librement accessibles sur Internet. » Elle* relève enfin « *que le traitement en cause concerne des données médicales, qui constituent des catégories particulières de données à caractère personnel, au sens de l'article 9 du Règlement. La nature de ces informations appelait donc une vigilance toute particulière afin d'éviter une violation de données. »*. Se faisant, elle rappelle au médecin, responsable de traitement, qu'un manque de vigilance contrevient au devoir de responsabilité lui incombant.

---

[32] Internet clandestin
[33] « Le GHT Coeur Grand Est touché par une cyberattaque », Tic Santé, 25 avril 2022
[34] Article 5 RGPD et article 6 LIL
[35]Délibération de la formation restreinte no SAN-2020-014 du 7 décembre 2020 & Délibération de la formation restreinte no SAN-2020-015 du 7 décembre 2020

Si elle n'a pas souhaité rendre publique l'identité des médecins, la CNIL a rendu publique la décision et souhaite ainsi acculturer les médecins au RGPD, mais aussi aux sanctions pécuniaires auxquels ils s'exposent en cas de manquement.

Le traitement des données de santé s'inscrit dans un cadre juridique en constante évolution, souvent mal ou méconnu des acteurs de la santé. Pour autant, en dépit de contraintes inhérentes à leur gestion comme ci-dessus appréhendées, ces données se révèlent nécessaires et utiles aux acteurs institutionnels tels que la HAS, les ARS, l'État, l'Assurance Maladie (§2). Le principe d'interdiction de traitement des données de santé ne saurait les dispenser de remplir leurs missions, sous la réserve que l'utilisation des données de santé par ces acteurs n'ait pour fins la promotion des produits de santé, l'exclusion de garanties des contrats d'assurance ou la modification des cotisations et des primes d'assurance.

§2 : L'utilisation des données de santé par les acteurs institutionnels : un traitement autorisé par la loi au titre des enjeux de santé publique

Il serait faux de croire que les autorités publiques n'encouragent pas le traitement des données de santé. Plus encore, l'accès et l'exploitation de ces données de santé touchent à la démocratie sanitaire et concourt à l'efficacité et à la transparence du système de santé. Il s'agit alors de nourrir l'élaboration, la conduite et l'évaluation des politiques publiques de santé, ainsi que le rappelle Jean-Marc Sauvé, vice-président du Conseil d'État dans son discours « Santé et Protection des données ».[37] De ce fait, l'on constate déjà les limites pratiques du principe d'interdiction du traitement des données de santé, qui ne peut prétendre à empêcher les organismes habilités à utiliser des données dans un objectif de maitrise médicalisée des dépenses de soins (*A*) ou de recherche (*B*).

A) La maitrise médicalisée des dépenses de soins grâce au traitement des données de santé

L'article 193 de la loi de modernisation de notre système de santé du 26 janvier 2016[38] est à l'origine de la création du Système national des données de santé (SNDS), un entrepôt de données médico-administratives dont le flux annuel représente 1,2 milliards de feuilles de

[37] Septièmes entretiens du Conseil d'État en droit social : Santé et protection des données Conseil d'État - Vendredi 1er décembre 2017.Introduction de Jean-Marc Sauvé, vice-président du Conseil d'État

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

soins, 11 millions de séjours hospitaliers, et 500 millions de données stockées. [39] Ce système, géré par la Caisse Nationale d'Assurance Maladie (CNAM) et la Plateforme de données de santé, Health Data Hub (HDH) regroupe en son sein, les données des hôpitaux à travers la base Programme de Médicalisation des Systèmes d'Information (PMSI), les causes médicales de décès à travers le Centre d'épidémiologie sur les causes médicales de décès (CépiDc), laboratoire de l'Inserm, les données relatives au handicap issues de Caisse Nationale de Solidarité pour l'Autonomie (CNSA) et certaines données des organismes complémentaires.

Aussi, le SNDS regroupe les données de l'assurance maladie de la base du Système national d'information inter-régime de l'Assurance maladie (SNIIRAM). Créé par la loi de financement de la sécurité sociale pour 1999 [40] avec la volonté d'un outil unifié de pilotage des dépenses de santé et créé, puis intégrée au SNDS en 2016, le SNIIRAM résulte d'une prise de consciences des pouvoirs publics quant à l'exploitation des données de santé et médico-administratives des assurances santé, lesquelles permettent « *d'identifier les effets bénéfiques ou délétères des politiques de santé, ou les effets indésirables extrêmement rares de thérapeutiques, lesquels ne sont pas identifiables dans des essais thérapeutiques contrôlés* ». [41] Une fois les craintes éthiques passées quant à la possible réutilisation des données, ce n'est qu'à partir de 2005 que l'entrepôt de données du SNIIRAM s'est enrichi à travers notamment des données issues des hospitalisations, des remboursements effectués par les caisses d'assurance maladie, et des référentiels de données sur les patients, sur la consommation de soins en ville, sur la consommation de soins en établissement, sur les pathologies traitées. Les limites fixées pour répondre aux craintes éthiques étaient d'exclure de ce traitement, les données résultant d'examen clinique ou paraclinique (tabagisme, niveau tensionnel etc.), les informations sur l'hospitalisation médico- sociale des personnes âgées ou sur les hospitalisations en long séjour, les informations médicales sur les séjours en centre hospitalier spécialisé (psychiatrie) et les données sociales (uniquement la notion de CMU-C était admise)[42]

Plus encore, le SNIIRAM, et aujourd'hui son successeur le SNDS, permettent de contribuer à la maitrise médicalisée des dépenses de santé, concept introduit par les ordonnances Juppé du

[39] Documentation du SNDS, "Qu'est-ce que le SNDS" https://documentation-snds.health-data-hub.fr/introduction/01-snds.html#a-quoi-le-snds-peut-il-servir
[40] Loi n° 98-1194 du 23 décembre 1998 de financement de la sécurité sociale pour 1999

[41] Fautrel B. « Base de données du SNIIRAM: l'ouverture de la boîte de Pandore », La Lettre du Rhumatologue, N° 439 - février 2018 p.4
[42] Rapport "Le SNIIRAM et les bases de données de l'Assurance Maladie en 2011 » Dominique POLTON, Philippe Ricordeau CNAMTS, 30 mars 2011

24 avril 1996[43], et ce à travers le traitement de données de santé. Concrètement, une cartographie met en lumière les actes ou médicaments spécifiques à des pathologies et remboursés par l'Assurance Maladie et dans un second temps, elle permet répartir les dépenses remboursées par l'Assurance Maladie selon les différentes pathologies, traitements et épisodes de soins repérés par les algorithmes. Ces dépenses remboursées représentent près de 167 milliards d'euros pour l'ensemble des régimes d'assurance maladie.[44] Cela permet d'aboutir à des données détaillées sur les consommations de soins et de contribuer à l'Objectif national de dépenses d'assurance maladie (Ondam) fixé par le Parlement.

D'un point de vue juridique, les autorités publiques ne se dispensent pas de l'interdiction du traitement des données de santé posé par la LIL et le RGPD mais bénéficient de l'application du régime de l'article 6 du RGPD. Ainsi, le SNDS justifie d'une base légale définie par la CNIL, comme ce qui autorise légalement la mise en œuvre d'un traitement et ce qui donne le droit à un organisme de traiter des données à caractère personnel. On peut également parler de « fondement juridique ». L'article 6 précise à ce titre que la mission d'intérêt public est une des six bases légales prévues et s'applique pour le SNDS. Le règlement n'a pourtant rien inventé, puisque déjà la loi du 26 janvier 2016 prévoyait que : « *Les données de santé à caractère personnel recueillies à titre obligatoire et destinées aux services ou aux établissements publics de l'État ou des collectivités territoriales ou aux organismes de sécurité sociale peuvent faire l'objet de traitements à des fins de recherche, d'étude ou d'évaluation présentant un caractère d'intérêt public* ».

Sur ce fondement, les chercheurs de l'Institut national de la santé et de la recherche médicale bénéficient d'un élargissement de l'accès aux données du SNDS *(B).*

B) L'élargissement de l'accès aux données du SNDS accordé à l'INSERM

La mission d'intérêt public est un fondement qui justifie un élargissement toujours plus large de l'accès aux données de santé. A ce titre, le décret dit SNDS du 29 juin 2021[45] accorde à l'INSERM une autorisation élargie d'accès permanent aux données du SNDS. De quoi continuer à interroger la pertinence du principe d'interdiction du traitement des données de santé, dont on peut penser qu'il est obsolète lorsque des missions de service public sont en

[43] Ordonnance no 96-346 du 24 avril 1996 portant réforme de l'hospitalisation publique et privée
[44] Chiffres 2021 de l'Assurance maladie.
[45] Décret n° 2021-848 du 29 juin 2021 relatif au traitement de données à caractère personnel dénommé « système national des données de santé »

jeu. En effet, avec l'entrée en vigueur de ce décret, les chercheurs de l'INSERM n'auront plus besoin d'une autorisation de la CNIL pour accéder aux principales données du SNDS et le feront sous la responsabilité de leur organisme, afin d'accélérer leurs projets de recherche.

C'est une avancée juridique majeure. Avant le décret SNDS, des méthodologies de référence (MR) en matière de recherche dans le domaine de la santé étaient définies par la CNIL, afin que le traitement des données de santé dans le cadre de recherches soit conforme au RGPD et à la LIL. Cette dernière prévoit par ailleurs que *« les traitements de données à caractère personnel à des fins de recherche, étude ou évaluation dans le domaine de la santé peuvent être mis en œuvre à condition que le responsable de traitement ait réalisé une déclaration de conformité à une méthodologie de référence. »* Deux MR avaient alors été définies : la MR-005 - Traitements de données du SNDS et des résumés de passage aux urgences (RPU) mis en œuvre par les responsables de traitements agissant dans le cadre de leur mission d'intérêt public et la MR-006 - Traitements de données du SNDS et des résumés de passage aux urgences (RPU) mis en œuvre par les responsables de traitements agissant dans le cadre de leurs intérêts légitimes..

L'intérêt public exigé par la CNIL pour autoriser l'accès aux données de santé du SNDS dans le cadre de recherches se comprend au regard de l'article 66 de la LIL *: « Les traitements relevant de la présente section ne peuvent être mis en œuvre qu'en considération de la finalité d'intérêt public qu'ils présentent. La garantie de normes élevées de qualité et de sécurité des soins de santé et des médicaments ou des dispositifs médicaux constitue une finalité d'intérêt public.* » L'article 1460-1 du CSP, modifié par la loi du 24 juillet 2019, a rajouté que de tels traitements *« ne peuvent avoir ni pour objet ni pour effet de porter atteinte à la vie privée des personnes concernées. Ils ne doivent en aucun cas avoir pour fin l'identification directe ou indirecte de ces personnes. »* L'intérêt légitime n'est quant à lui pas défini par les textes, mais la CNIL en fournit une explication : le responsable de traitement des données de santé doit « opérer une pondération entre son intérêt et les « intérêts ou libertés et droits fondamentaux des personnes » et doit également intégrer les « attentes raisonnables » de ces personnes.

En tout état de cause, les MR 0005 et 006 était réservées à certains acteurs et portaient sur un périmètre des seules données du programme de médicalisation des systèmes d'information (PMSI). A la suite d'une consultation publique, ne s'opposant pas à l'autorisation d'un accès permanant aux données du SNDS pour l'INSERM, la CNIL a permis la suppression du régime d'autorisation.

A titre d'illustration, le projet BACTHUB a vu le jour, issu d'une collaboration entre l'AP-HP et l'INSERM. Il permet de mieux comprendre le lien entre prise d'antibiotiques et le développement ultérieur d'une infection à bactérie résistante aux antibiotiques. Concrètement, ce sont des données inédites de 50 000 patients, issues de 37 hôpitaux sur 5 ans, qui ont été consolidées en un an avec l'appui d'ingénieurs du Health Data Hub[46], la plateforme qui regroupe les données de santé comprises dans le SNDS. Le projet BACTHUB souhaite répondre au problème de santé publique que représente la diffusion de bactéries résistantes aux antibiotiques dans la population.

Cette première section permet de souligner le cadre juridique du traitement des données de santé, largement articulé autour du principe d'interdiction. Elle souligne également la possibilité pour les acteurs institutionnels, dans l'intérêt public, d'utiliser des données médicales aux fins de leurs activités. Ceux-ci se tournent vers l'Institut national des données de santé (INDS), point d'accès aux données de santé créé en 2007.
La majeure partie des données de santé sont récoltées lors de prises en charge par les professionnels exerçant dans les établissements de santé ; la section 2 sera consacrée l'étude de ce cas d'usage des données de santé (Section II).

Section II: Le traitement des données de santé au sein de l'établissement de santé

Dès que le patient passe le seuil d'un établissement de santé, des données personnelles dont des données de santé sont collectées pour sa prise en charge et son admission. Il incombe à la structure de soins de s'assurer que le traitement est conforme à la réglementation relative à la protection des données personnelles de santé (§1), elle doit également agir au regard de l'obligation faite à tout professionnel de santé de disposer de données à même d'assurer une prise en charge et une continuité des soins au patient (§2)

§ 1 : Un traitement conforme des données de santé incombant à l'établissement de santé: respect du RGPD et accompagnement par l'État

Depuis le 25 mai 2018, date d'entrée en application du RGPD, chaque établissement, public ou privé, étant donné qu'il traite des données de santé, doit répondre à certaines obligations, principes et mesures afin d'être en conformité avec le Règlement.

[46] Article L 1462-1 du CSP, modifié par la loi n° 2019-774 du 24 juillet 2019 relative à l'organisation et à la transformation du système de santé

Il donc fallu prendre la mesure de deux exigences : le cumul des articles 6 et 9 du RGPD pour légitimer le traitement *(A)* et le rôle de l'État dans la conformité attendue des acteurs de la santé *(B).*

A) L'exigence d'un cumul des articles 6 et 9 du RGPD permettant le traitement des données de santé

L'article 6 du RGPD pose six bases légales, alternatives, autorisant le traitement de données à caractère personnel, à condition qu'un de ces fondements juridiques le justifie. Il s'agit de la sauvegarde des intérêts vitaux lorsque le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée, ou d'un tiers ; du consentement, la personne a consenti au traitement de ses données ; du contrat qui rend le traitement nécessaire à l'exécution ou à la préparation d'un contrat avec la personne concernée ; l'obligation légale, cas dans lequel le traitement est imposé par des textes légaux ; la mission d'intérêt public qui signifie que le traitement est nécessaire à l'exécution d'une mission d'intérêt public et l'intérêt légitime rendant le traitement nécessaire à la poursuite d'intérêts légitimes de l'organisme qui traite les données ou d'un tiers, dans le strict respect des droits et intérêts des personnes dont les données sont traitées.

A l'hôpital, le traitement des données de santé n'est pas un tabou juridique. C'est sur la base de l'intérêt public que les établissements public de santé traitent les données des patients (l'usager du service public hospitalier se trouve en effet dans une situation dite « *légale et réglementaire* »). Cet intérêt public peut s'analyser à la lecture conjointe de deux articles du CSP : l'article L 1110-1 garantissant le droit fondamental à la protection de la santé et qui dispose que *« Les professionnels et les établissements de santé (…) participant à la prévention, aux soins ou à la coordination des soins contribuent (…) à développer la prévention, garantir l'égal accès de chaque personne aux soins nécessités par son état de santé et assurer la continuité des soins et la meilleure sécurité sanitaire possible* » ainsi que l'article L 6111-1 listant les missions des établissements de santé.
Ainsi, l'établissement de santé collecte, génère et traite également des données de santé pour remplir ses obligations de prise en charge sanitaire et de continuité des soins. Il se base sur un des six fondements juridiques de l'article 6 du RGPD, auquel on cumule une exception au principe d'interdiction du traitement des données de santé de l'article 9.

Ainsi, l'article 9 du RGPD dispose que le traitement des données à caractère personnel qui révèle l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique sont interdits. En son point h, il émet une exception lorsque *« le traitement est nécessaire aux fins de la médecine préventive ou de la médecine du travail, de l'appréciation de la capacité de travail du travailleur, de diagnostics médicaux, de la prise en charge sanitaire ou sociale (...) »*. Cela se rapporte aux activités des établissements des secteurs sanitaire, social et médico-social mentionnées dans la loi, mais aussi aux missions des services de santé au travail et de médecine préventive.

A cette exigence de cumul des articles 6 et 9 du RGPD, l'on rattache alors la finalité du traitement des données de santé. Ainsi, dans une notice d'information à destination de ses patients, le CHU de Rouen identifie trois finalités justifiant la récolte des données : la prise en charge médicale et administrative, les traitements obligatoires du fait de la réglementation tels que l'évaluation des pratiques professionnelles et la gestion des évènements indésirables et l'amélioration de la qualité des soins et des services dans un but de satisfaction. [47]

Le développement du numérique dans les établissements de soins et l'exigence de conformité au RGPD qui en découle, s'est accompagné d'un nécessaire soutien de l'État (*B*).

B) Le rôle de l'État dans la conformité au RGPD des établissements de santé : accompagnement au virage du numérique en santé

Afin d'accompagner les acteurs de la santé dans la conformité aux exigences du RGPD, l'État s'est doté de moyens humains et matériels au service du numérique en santé. Le Parlement a également soutenu cette transition par le vote de lois. Ainsi que le rappelle Bénédicte Bévière-Boyer, «*Les autorités françaises, juridiquement responsables de la politiques de santé publique, doivent assurément garantir aux citoyens français la protection effective de leurs données »*. [48]

En 2018, le président de la République Emmanuel Macron annonçait le plan de transformation du système de santé « Ma santé 2022 ». L'objectif assumé était de moderniser

[47] « Notice d'information relative à la protection des données personnelles sur les données de santé vous concernant pour les soins et la recherche », CHU Rouen Normandie

[48] Bévière-Boyer, Bénédicte. « La protection des données de santé mises à disposition par le Health Data Hub pour les recherches sur la Covid-19 », Journal du Droit de la Santé et de l'Assurance - Maladie (JDSAM), vol. 29, no. 2, 2021, pp. 37-48.

le parcours de soin en France pour améliorer le parcours patient, véritable enjeu de santé publique. L'ambitieuse feuille de route du numérique en santé comptait parmi ses objectifs le déploiement en 2022 de l'Espace numérique en santé (ENS) ainsi que le déploiement de la télémédecine, parachevé par l'avenant 9 à la Convention médicale[49].

Pour accompagner les établissements à la suite de l'entrée en vigueur du RGPD, quatre interventions majeures de l'Etat sont à relever, de nature différente :

- Soutien financier : pour répondre aux enjeux de sécurité posés par le traitement des données de santé, l'État Français a débloqué un milliard d'euros pour renforcer la sécurité informatique, entre autres, des hôpitaux (financé par France Relance et le Programme d'investissement d'avenir).
- Intervention législative : le législateur a organisé l'hébergement de données de santé (HDS), qui a pour but d'encadrer la conservation et la restitution des données de santé, dans des conditions propres à garantir leur confidentialité et leur sécurité. Ainsi, est imposée une certification dite « HDS », dont les conditions de délivrance sont fixées par décret en Conseil d'État, pris après avis de la CNIL et des conseils nationaux de l'ordre des professions de santé. Cela intervient en complément du cadre fixé par la loi Kouchner du 4 mars 2002, qui avait constitué le socle de la réglementation applicable à l'hébergement de données de santé, en introduisant dans le CSP l'article L.1111-8.
- La Direction Générale de l'Offre de Soins (DGOS) a lancé en février 2021 le programme HOP'EN (« Hôpital Numérique Ouvert sur son Environnement ») plan d'action national des systèmes d'information hospitaliers. Selon le site du Ministère de la santé, le programme « *a comme ambition d'amener - d'ici 2022 - les établissements de santé, quels que soient leur statut, leur taille et leur activité, à un palier de maturité de leur système d'information, nécessaire pour répondre aux nouveaux enjeux de décloisonnement du système de santé et de rapprochement avec les patients.* » et ceci, en étroit lien avec les nouvelles exigences du RGPD.
- Dans le cadre du Ségur du numérique en santé, dont l'ambition était de généraliser et de sécuriser le partage fluide des données de santé entre professionnels, deux milliards d'euros ont été investis pour soutenir le déploiement massif du numérique en santé. Le Ségur de la santé, en déployant des services socles a permis d'accélérer la mise en conformité au RGPD d'établissements de santé en les incitant à faire preuve de

[49]Arrêté du 22 septembre 2021 portant approbation de l'avenant n°9 à la convention nationale organisant les rapports entre les médecins libéraux et l'assurance maladie signée le 25 août 2016

vigilance et de sécurité dans le traitement des données de santé. L'on citera par exemple : l'Identité Nationale de Santé (INS), obligatoire depuis janvier 2021 et permettant de référencer les données de santé afin d'éviter toute erreur d'identification des personnes prises en charge ; ou Pro Santé Connect (PCS) permettant de sécuriser l'accès des systèmes d'information hospitaliers aux seules personnes habilitées.

Le traitement des données de santé en établissement, devant répondre aux exigences croisées du RGPD, de la LIL et des dispositions du CSP est la résultante d'une obligation de recueil des données de santé faite aux professionnels de santé, dans l'exercice de leur pratique (§2).

§2 : L'obligation de recueil des données de santé faite à tout professionnel de santé : condition de la prise en charge du patient

Cette obligation se traduit par la tenue d'un dossier patient (*A*) et est encadrée par des procédures de sécurité informatique, répondant aux besoins d'utilisation par les professionnels des outils de l'e-santé (*B*).

A) L'obligation de tenue et de conservation d'un dossier patient : un exemple de traitement de données de santé

Les médecins et les établissements de soins sont tenus de tenir un dossier patient, recensant les informations médicales, administratives, paramédicales de ce dernier, indépendamment de son lieu de prise en charge (ES, EHPAD, cabinet de ville, milieu professionnel). Le dossier « médical » est, quant à lui, constitué pour chaque hospitalisation.

Son contenu est fixé par l'article R 1112-2 du CSP, lequel prévoit que le dossier médical doit contenir *« les informations formalisées recueillies lors des consultations externes dispensées dans l'établissement, lors de l'accueil au service des urgences ou au moment de l'admission et au cours du séjour hospitalier, les informations formalisées établies à la fin du séjour ainsi que les informations mentionnant qu'elles ont été recueillies auprès de tiers n'intervenant pas dans la prise en charge thérapeutique ou concernant de tels tiers. »*

Dans le sens inverse, « *le patient doit l'information nécessaire à sa prise en charge médicale au médecin qui le traite soit au titre du contrat de soins privé, soit au titre de l'obligation de l'usager au regard du fonctionnement du service public. La constitution du dossier médical n'est pas que la formalisation de cette obligation du malade »* [50]

[50] DAUBECH L. "La collecte des données de santé" RGDM 2004 NS Droit des données de santé, p45

A cette obligation, s'ajoute celle de conserver le dossier patient et les données personnelles le composant. En effet, la conservation des dossiers peut constituer un moyen de preuve en cas recherche de la responsabilité du médecin, permet d'assurer la continuité des soins et de répondre à une demande de communication du dossier par le patient. Sur ce dernier point, la CNIL a sanctionné d'une amende de 10 000 €, un cabinet dentaire ne coopérant pas avec la Commission et refusant abusivement la communication de son ancien dossier à un patient.[51]
Se pose alors la question de la durée de conservation et de son responsable.
L'article R 1112-7 du CSP, de par sa longueur et son manque de lisibilité, apporte une première réponse « *Les informations concernant la santé des patients sont soit conservées au sein des établissements de santé qui les ont constituées, soit déposées par ces établissements auprès d'un hébergeur dans le respect des dispositions de l'article L. 1111-8.* »
Une option entre la conservation en interne et l'externalisation à un hébergeur est donc laissée aux établissements de santé.

Puis, l'article R 1112-7 pose plusieurs délais de conservation du dossier médical, comme s'il revenait à l'établissement de santé de choisir les différentes options qui s'offrent à lui *: « le dossier médical (…) est conservé pendant une durée de vingt ans à compter de la date du dernier séjour de son titulaire dans l'établissement ou de la dernière consultation externe en son sein. Lorsqu'en application des dispositions qui précèdent, la durée de conservation d'un dossier s'achève avant le vingt-huitième anniversaire de son titulaire, la conservation du dossier est prorogée jusqu'à cette date. Dans tous les cas, si la personne titulaire du dossier décède moins de dix ans après son dernier passage dans l'établissement, le dossier est conservé pendant une durée de dix ans à compter de la date du décès. (…)* »
Le délai de droit commun est de vingt années pour une personne majeure, mais ne s'applique pas au DMP, conservé seulement dix ans. L'article ne le précise pas. Le décès du patient et son âge changent la donne. S'il décède moins de 10 ans après son dernier passage dans l'établissement, le dossier est conservé pendant une durée de 10 ans à compter de la date du décès. En revanche, s'il est mineur au moment de son passage dans l'établissement, il est recommandé par les Ordres des médecins de le conserver vingt-huit ans.
La responsabilité de la conservation des données du dossier médical revient à l'établissement de santé dont le directeur veille à ce que tout soit mis en œuvre pour assurer la garde et la

[51] Délibération CNIL, n° SAN-2017-008, 18 mai 2017

confidentialité des informations ainsi conservées ou hébergées. En réalité, cette « veille » revient à la Direction des systèmes d'information (DSI) soutenue par le rôle du délégué à la protection des données. Ces deux acteurs ont vu leurs rôles devenir indispensables au sein des établissements de santé, en raison des cyberattaques et fuites de données de plus en plus fréquentes.
QUID in fine des dossiers médicaux de patients pris en charge en cabinet libéral ? Le Conseil National de l'Ordre des médecins (CNOM) est intervenu et recommande aux médecins d'appliquer les délais de conservation prévus pour les établissements de santé.

Cette généralisation du traitement informatique des dossiers médicaux et leur conservation désormais également informatisée, imposent de fait, des procédures de sécurité informatique dans les établissements de santé *(B),* obligeant les professionnels à s'adapter et à faire preuve de davantage de vigilance.

B) Les procédures de sécurité informatique dans les établissements : une réponse technique à la sensibilité des données de santé

A l'occasion de la publication du Référentiel d'identification électronique à destination des acteurs des secteurs sanitaire, médico-social et social[52], l'ANS rappelait que « *la manière dont on se connecte à un service numérique en santé est essentielle, à la fois pour développer les usages et pour renforcer la sécurité des données de santé.* » [53] A ce titre, les services numériques en santé sont définis par l'article L 1470-1 du CSP comme « les *systèmes d'information ou les services ou outils numériques mis en œuvre par des personnes physiques ou morales de droit public ou de droit privé, y compris les organismes d'assurance maladie, proposés par voie électronique, qui concourent à des activités de prévention, de diagnostic, de soin ou de suivi médical ou médico-social, ou à des interventions nécessaires à la coordination de plusieurs de ces activités.* » Mais, le Code n'en donne pas une liste exhaustive, laissant de la marge à l'ANS et au Ministère de la santé et des solidarités pour établir ensemble un socle de services considérés comme tels : télésanté, portails patients, dossier médical partagé (DMP), déclaration en ligne des décès (Cert-DC) et de maladies à déclaration obligatoire (E-DO) etc.

[52] PGSSI-S Référentiel d'identification électronique Acteurs des secteurs sanitaire, médico-social et social [personnes physiques], 01 avril 2022, Agence du Numérique en santé
[53] Communique de presse de l'ANS, « Un grand pas pour la sécurité et les usages du numérique en santé : publication du référentiel sur l'identification électronique », 01 avril 2022

L'objectif de ces services est de soutenir les professionnels dans leur pratique médicale et de favoriser les échanges de données de santé pour la coordination des soins, au bénéfice du patient. La protection de ces échanges restant majeure, des procédés de sécurité informatique sont adoptés sous la forme de référentiels.

Dernièrement, pris en application des dispositions des articles L. 1470-2 et L. 1470-5 du CSP[54] et du règlement eIDAS de 2014, l'arrêté du 28 mars 2022[55] approuve le référentiel sous la forme de trois volets consacrés aux usagers, aux professionnels des secteurs sanitaire, médico-social et social et aux personnes morales relevant de ces secteurs.
Le référentiel, pour le volet destiné aux professionnels de santé, exige un niveau de garantie minimum lorsqu'ils s'identifient électroniquement lors de leur usage des services numériques en santé. Il souhaite « *trouver le juste équilibre entre, d'une part, la nécessaire sécurité dans le traitement des données de santé et, d'autre part, la réalité des usages par les professionnels qui prennent en charge les patients* »[56] . Dès lors, l'usage d'une identité numérique (fourni par Pro-santé connect, un service mis à disposition par l'ANS) pour les professionnels n'est plus seulement recommandée, mais devient obligatoire au 1er janvier 2023 et permet de se connecter via l'application mobile e-CPS et les cartes professionnelles de santé (CPS) aux services numériques en santé. Les CPS ont aujourd'hui la possibilité d'être dématérialisées, avec la volonté pour la puissance publique de faciliter l'usage du numérique en santé pour les professionnels.
Ces exigences renforcées de sécurités sont mises en œuvre avec pédagogie, puisque le référentiel décrit des paliers à atteindre entre juin 2022 et décembre 2025 ; laissant une marge aux professionnels de santé pour s'équiper et adapter leur pratique aux exigences qu'imposent le traitement des données de santé.

[54] Création Ordonnance n° 2021-581 du 12 mai 2021 relative à l'identification électronique des utilisateurs de services numériques en santé et des bénéficiaires de l'assurance maladie
[55] Arrêté du 28 mars 2022 portant approbation du référentiel relatif à l'identification électronique des acteurs des secteurs sanitaire, médico-social et social, personnes physiques et morales, et à l'identification électronique des usagers des services numériques en santé
[56] Communique de presse de l'ANS sus-cité

Ce premier chapitre permet de mettre en exergue d'une part le difficile respect du principe d'interdiction du traitement des données de santé, et d'autre part la nécessité pour les établissements et professionnels de santé ainsi que pour les organismes en lien avec la santé, de les traiter. La conciliation entre la vie privée des personnes, leur prise en charge sanitaire conditionnée au partage de leurs données et la protection de celles-ci est un défi dont les pouvoirs publics ont pris conscience. Les objectifs de sécurité à remplir pour garantir l'intégrité et la confidentialité des données de santé sont un impératif pour les responsables de traitement ainsi que pour les professionnels utilisateurs d'outils d'e-santé. Mesure en a été prise au vu de l'important corpus juridique encadrant la question.

Il est donc primordial de prendre avec recul l'interdiction de traiter les données de santé, puisqu'elle n'est qu'une interdiction sous exceptions, comme une disposition pensée tout en sachant qu'elle serait contournée.

Mais, alors qu'elles s'avèrent être le fruit de l'intimité de la personne, il est frappant de constater que les données de santé sont la plupart du temps, traitées sans le consentement de la personne concernée. Plus encore, l'article 9 du RGPD organise la levée de l'interdiction du traitement des données de santé si « *la personne concernée a donné son consentement explicite au traitement de ces données à caractère personnel pour une ou plusieurs finalités spécifiques* »[57]. S'en suivent d'autres exceptions, comme l'intérêt public traité ci-dessus. Mais la première d'entre elle demeure le consentement. Que faut-il en déduire ? Que le patient entrant dans l'établissement devrait consentir à ce que l'on recueille ses données tout le long de sa prise en charge ? Qu'il devrait le faire à chaque fois que des médecins échangent des informations à son sujet ? Que l'hôpital ne pourrait transmettre les informations relatives à son séjour uniquement après le recueil d'un consentement clair et éclairé ? La pratique rend cette exception difficilement applicable, et donc marginale. Cela est difficile à appréhender alors même que la sensibilité des données partagées pourrait justifier la formulation d'un consentement du patient à chaque étape de sa prise en charge.

Le chapitre qui suit œuvrera à démontrer que le consentement, exception au principe d'interdiction du traitement des données de santé, n'est, sauf dans des cas particuliers comme la recherche médicale, ni simple à appliquer, ni même pertinente au regard de la pratique en établissement de soins (Chapitre II).

---

[57] Article 9 du RGPD, point 2 a - Traitement portant sur des catégories particulières de données à caractère personnel

Chapitre II : Le consentement du patient comme exception au principe d'interdiction du traitement des données de santé

« Le consentement est l'accord de deux ou plusieurs volontés, en vue de créer des effets de droits ». [58]

Le consentement est l'un des six fondements juridiques (ou bases légales) justifiant la licéité du traitement de données (ce qui autorise légalement sa mise en œuvre). En plus, le consentement exprès de la personne constitue une exception au principe d'interdiction du traitement des données de santé (article 9.a du RGPD). La relation entre l'article 6 et l'article 9 du RGDP n'a pas été clarifiée dans l'enseignement et la pratique. Néanmoins, il est d'avis que l'autorisation du traitement des données est donnée par l'article 6§1 du RGPD (base légale) et cumulée par une exception au principe d'interdiction à l'article 9, paragraphe 2 du RGDP.

Renforcé par le RGPD, le consentement du patient était déjà inscrit dans la loi de 1978 et dans la directive de 1995, en tant que base légale mais aussi en tant qu'exception au principe d'interdiction. C'est ce dernier point qui sera appréhendé dans le chapitre 2, au travers d'une première section sur les nuances à apporter au consentement du traitement des données de santé et d'une seconde sur l'impérative nécessité de disposer d'autres exceptions que le consentement pour traiter les données de santé.

[58] CORNU G. Vocabulaire juridique, Paris, association Henri Capitant, PUF-Quadrige, 2016, p 245

Section I : Le consentement, une exception à nuancer à la lueur des enjeux du traitement des données de santé

Longtemps, le consentement a été tenu pour secondaire dans la conception qui prévalait de la relation du médecin et du patient. Non seulement le consentement explicite n'était pas requis, mais plus encore, l'information ne l'était pas davantage. Le terme « *consentement* » doit son essence au droit civil des contrats. L'article 1108 du Code civil de 1804 en fait l'une des conditions essentielles de la validité d'une convention.

Le consentement a par la suite émergé en droit de la santé, et plus récemment en droit du numérique, parallèlement à son essor. Il est aujourd'hui requis lors de certains traitements de données, mais présente dans la pratique, des limites (§1). Le recueil du consentement du patient au traitement de ses données de santé prend finalement son sens dans le cadre de l'échange et du partage d'informations entre professionnels de santé (§2).

§1 : Les limites formelles du consentement du patient au traitement de ses données de santé

Le consentement du patient, en état d'exprimer sa volonté est nécessaire à la réalisation d'un acte ou d'un traitement médical. Au cœur de la confiance en la médecine, ce consentement peut être confondu avec le consentement au sens du RGPD, portant sur le traitement des données de santé. Une distinction est alors à opérer (*A*), avant de constater les limites du consentement au traitement des données de santé dans la pratique des professionnels (*B*).

A) Une distinction nette entre consentement à l'acte médical et consentement au traitement des données de santé

Depuis l'arrêt Teyssier du 28 janvier 1942[59] et la loi du 4 mars 2002 relative aux droits des patients, le consentement, corolaire de la dignité de la personne, est devenu la clé de voûte de la relation médecin-patient et la « *légitimation première de l'acte médical* »[60]. Comme le précise l'article L. 1111-4 du Code de la santé publique : « *Aucun acte médical ou aucun traitement ne peut être pratiqué sans le consentement libre et éclairé de la personne*. »

L'article 4 point 11 du RGPD énonce que « *le consentement de la personne concernée par le traitement informatique de ses données de santé, signifie toute manifestation de volonté libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une*

[59] 28 janvier 1942, chambre des requêtes de la Cour de cassation (DC 1942. 63 ; Gaz. Pal. 1942. 1. 177)
[60] Expression du Professeur Olivier Guillod en 2014

déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement. » Déjà inscrit dans la LIL, ce consentement a été renforcé. Il permet de contourner l'interdiction de principe du traitement des données de santé, si *« la personne concernée a donné son consentement explicite au traitement de ces données à caractère personnel pour une ou plusieurs finalités spécifiques, sauf lorsque le droit de l'Union ou le droit de l'État membre prévoit que l'interdiction visée au paragraphe 1 ne peut pas être levée par la personne concernée »*[61]. Pour autant, le CSP et le RGPD insistent sur le caractère éclairé du consentement, particulièrement important en ce que le patient dispose d'un droit à une information loyale, claire et appropriée, lors de sa prise en charge médicale mais aussi lors de l'utilisation de ses données de santé. Ainsi, avant d'obtenir le consentement de la personne concernée, celle-ci doit être parfaitement informée sur les finalités de la démarche, à savoir l'usage fait de ses données et la durée de leur conservation.

Le consentement qui permet de déroger à l'interdiction du traitement des données de santé doit être explicite ; un consentement tacite ne suffira pas. Selon les lignes directrices 5/2020[62] du Comité Européen de la Protection des Données (CEPD), le RGPD préconise des déclarations écrites et signées dans toutes les situations où un consentement explicite valable est nécessaire et nous donne un exemple valant consentement explicite dans le domaine de la chirurgie esthétique : « *une clinique de chirurgie esthétique demande le consentement explicite d'un patient afin de transférer son dossier médical à un expert consulté dans le but d'obtenir une deuxième opinion sur l'état du patient. Le dossier médical se présente sous la forme d'un fichier numérique. Au vu de la nature spécifique des informations concernées, la clinique demande la signature électronique de la personne concernée afin d'obtenir un consentement explicite valable et d'être en mesure de démontrer qu'un consentement valable a été obtenu ».*

Dès lors, un professionnel de santé pourrait-il se dispenser de recueillir le consentement au traitement des données de santé d'un de ses patients, sous le prétexte que ce dernier a déjà donné son consentement à l'acte médical ? Autrement dit, peut-on considérer que le patient pris en charge, consent par la même occasion à l'utilisation de ses données de santé ? L'information qui lui est délivrée lors de l'explication de l'acte médical qu'il va subir englobe-t-elle l'information sur le traitement des données de santé ? La réponse à ces multiples interrogations est négative car la loi distingue explicitement le consentement au sens

[61] Article 9. 2 point a du RGPD
[62] Lignes directrices 5/2020 sur le consentement au sens du règlement (UE) 2016/679

médical, du consentement au sens du RGPD supposant qu'un traitement informatique soit effectué sur les données recueillies.

De surcroit, la preuve du consentement à l'acte médical est distincte de celle du consentement au traitement de ses données de santé. À l'article 7 paragraphe 1, le RGPD souligne l'obligation explicite du responsable du traitement de démontrer que la personne concernée a donné son consentement. En vertu de cet article, la charge de la preuve reposera donc sur l'établissement ou le professionnel de santé qui utilise les données. Une obligation méconnue en pratique, car force est de constater que l'usage du terme « consentement » au traitement des données de santé peut conduire le professionnel - peu informé – à le confondre avec le consentement de l'article L 1111-4 du CSP. Mais, le consentement du RGPD n'est pas le consentement à l'acte médical, et porte un objet bien différent qu'est la pratique médicale.

Il a été démontré ci-dessus que la recherche du consentement avant chaque traitement de données de santé est impossible. Déjà la directive 95/46[63] prévoyait un contournement de ce consentement au travers de deux exceptions : lorsque des raisons d'intérêt général le justifiaient, en particulier, à des fins de santé publique ou si cela était nécessaire pour protéger les intérêts vitaux de la personne concernée ou d'une autre personne lorsque la personne concernée est physiquement ou juridiquement incapable de donner son consentement. Le RGPD a repris ces possibilités, conservées également dans la loi Informatiques et Libertés. Le tout-consentement n'est donc pas la règle en matière de protection des données à caractère personnel.

Le consentement en droit des données de santé n'a pas la même résonance qu'en droit de la santé, et n'est pas un principe exalté et tout aussi solide. Dans la pratique médicale, il présente même des limites qu'il s'agira de contourner dans l'intérêt de la santé (*B*).

B) Le recours au consentement dans le traitement des données de santé : limites rencontrées par les professionnels de santé

Le recours à l'exception du consentement pour traiter les données de santé pose des contraintes. En effet, la critique faite au cadre juridique actuel sur la protection des données personnelles est que « *le consentement - bien qu'il soit explicite et informé- ne reflète pas les*

[63]Directive 95/46/CE du Parlement européen et du Conseil, du 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

intérêts réels des individus»[64], c'est-à-dire que notre possibilité de consentir serait remise en cause par l'impossibilité de faire autrement dans une société hyper-numérisée.

Dans le domaine de la recherche, le recueil du consentement au traitement des données de santé peut s'avérer délicat, puisque les suites et les risques ne sont pas toujours connus ; et surtout les données peuvent être exploitées à de multiples reprises. En effet, selon le CCNE[65], « *le consentement – du patient - au recueil et à l'utilisation des données personnelles sont rendus plus complexes dès lors que les données peuvent être aisément dupliquées et réutilisées à des fins non initialement définies et que leur traitement fera apparaître de nouvelles données, dites secondaires, souvent plus sensibles que les données initiales* ».

Pour solution et afin de favoriser l'utilisation des données médicales pour la recherche, les Hôpitaux Universitaires de Genève (HUG), ont développé un formulaire électronique de consentement pour les patients[66], conjointement conçu par les équipes médicales concernées et la Direction des systèmes d'information des HUG. Le projet a été soutenu par la Fondation Privée des HUG et permet de recueillir plus rapidement et aisément le consentement du patient pour traiter ses données de santé. Pour autant, le risque est de moduler à la baisse le standard du professionnel que l'on attend en termes d'obligation d'information, car un consentement électronique ne le dispense pas d'informer sur le traitement dont feront l'objet les données du patient se prêtant à la recherche.

Pourtant, les données des patients sont précieuses au développement de projets de recherche médicale. Selon Stéphanie Combes, *« la data devient la clé d'une médecine à la fois plus prédictive par rapport au parcours de soins du patient, plus précise pour définir le choix du bon traitement au bon moment et plus personnalisée pour cibler les profils de patients susceptibles d'y répondre favorablement. »*[67] La création du Health Data Hub répond à cet objectif. Créé par la Loi du 24 juillet 2019, le HDH est une structure publique dont l'objectif est de permettre aux porteurs de projet d'accéder facilement à des données non nominatives accessibles sur une plateforme sécurisée, dans le respect de la réglementation et des droits des citoyens. Récemment, six projets de recherche ont été sélectionnés dans le cadre d'un Appel à

[64]Bourcier, D., De Filippi, P. (2018). Vers un droit collectif sur les données de santé. In Revue de droit sanitaire et social (RDSS), Dalloz Revues, 2018 (n.3) pp. 444-456
[65] Avis 130 du CCNE, Données massives et santé : une nouvelle approche des enjeux éthiques, 29 mai 2019
[66] Annexe 1
[67]Article extrait du dossier Grand Angle spécial Innovation en santé, CommEditions, parution dans Le Monde daté du 23 avril 2022.

Manifestation d'Intérêt lancé par le HDH et le Ministère de la santé au printemps 2021. Les chercheurs auront accès aux données de santé de la plateforme. Parmi eux, le « D-IA-GNO-DENT » porté par le Professeur Bloch-Zupan des Hôpitaux Universitaires de Strasbourg, qui souhaite à travers le traitement croisé de données de santé, développer l'intelligence artificielle au soutien de l'aide au diagnostic de maladies rares à expression bucco-dentaires. Dans ce cas de figure, le consentement au traitement des données de santé des patients ne sera pas requis, car les données ne permettent pas de remonter à la personne. La LIL impose alors une obligation d'information individuelle, que le RGPD complète par une information générale qui permet aux personnes d'exercer les droits reconnus par le RGPD et notamment le droit d'opposition.

Le consentement n'est pas tout et dans la recherche, le RGPD aménage une exception permettant de contourner le principe d'interdiction du traitement des données de santé, et qui peut être rattachée au fondement juridique (article 6) de l'intérêt public. Ainsi, le point i de l'article 9 du RGPD dispose que « *le traitement est nécessaire pour des motifs d'intérêt public dans le domaine de la santé publique, tels que la protection contre les menaces transfrontalières graves pesant sur la santé, ou aux fins de garantir des normes élevées de qualité et de sécurité des soins de santé et des médicaments ou des dispositifs médicaux, sur la base du droit de l'Union ou du droit de l'État membre qui prévoit des mesures appropriées et spécifiques pour la sauvegarde des droits et libertés de la personne concernée, notamment le secret professionnel* » L'on constate alors, que le consentement n'est pas l'exception sur laquelle l'on s'appuie pour l'accès aux données dans la recherche médicale, mais que l'intérêt public, c'est-à-dire celui de la société prime.

En revanche, dans le domaine de l'échange et du partage de données, le consentement du patient peut-être un préalable en fonction de l'appartenance du professionnel à l'équipe de soins (§2). En tout état de cause, cela reste un enjeu important de santé publique dans la mesure où l'accès aux données de santé du patient entre professionnels permet de lui garantir un parcours de soins cohérent.

§2 : Le consentement au partage et à l'échange de données entre professionnels de santé : un enjeu pour l'accès aux données de santé

Le consentement au traitement des données de santé trouve véritablement sa place dans l'échange et le partage entre professionnels, au service de la coordination des soins et des parcours patients (*A*).

Ce consentement a nécessité des précisions législatives lorsqu'il est requis hors équipe de soins. Mais, que le partage intervienne en ou hors équipe de soins, le secret professionnel reste la règle et permet de sécuriser les données de santé (*B*).

A) L'échange et le partage des données de santé pour une meilleure coordination des parcours et des soins

Le Dossier Médical Partagé (DMP) est l'illustration de l'échange et du partage des données de santé. Crée par la loi du 13 août 2004[68] et initialement appelé « *dossier médical personnel* », il est un relatif échec dans un premier temps, car ne reçoit pas un plébiscite unanime des acteurs censés l'utiliser. Le DMP renaît en 2016 à travers la loi du 26 janvier[69], sous le nom de Dossier médical partagé. Précisément, la loi Touraine a souhaité mettre l'accent sur le partage des données de santé du patient, en soutien à une meilleure coordination des soins. La ministre de la santé de l'époque, Mme Touraine s'était exprimée en ce sens devant l'Assemblée Nationale lors du vote de la loi : « *Nous relançons le DMP (…) en mettant l'accent sur le partage de l'information (…). C'est à cette condition que les coopérations et les équipes de soins primaires pourront effectivement fonctionner* ». [70] Six ans après sa renaissance, le DMP échoue à nouveau, et n'est pas alimenté par les professionnels. Il est refondu depuis 2022, dans « Mon espace santé »[71] (MES), outil numérique qui permet aux utilisateurs, de gérer leurs données de santé et de participer à la construction de leur parcours de soin.

L'échange et le partage de données de santé entre professionnels sont deux notions distinctes, disposant de leur propre régime juridique, depuis une intervention législative clarifiant ces deux mécanismes. Ainsi, la loi MNSS de 2016 et le décret d'application du 20 juillet 2016 précisent que l'échange de documents comportant des données de santé consiste dans un flux de données visant à communiquer des données de santé à un (des) destinataire(s) clairement identifié(s). Par exemple, cela concerne l'envoi d'un mail par messagerie sécurisée de santé. Le partage vise à mettre à la disposition de plusieurs professionnels fondés à les connaître, des données de santé utiles à la coordination et à la continuité des soins, dans l'intérêt de la

[68] Loi n°2004-810 du 13 aout 2014 relative à l'assurance maladie

[70] Loi du 26 janvier 2016, dossier législatif assemblée nationale, débats: www.assemblée-nationale.fr/14/dossiers/santé.asp
[71] Décret n° 2021-1048 du 4 août 2021 relatif à la mise en œuvre de l'espace numérique de santé

personne prise en charge. C'est l'exemple des informations disponibles dans le Dossier Pharmaceutique (DP) ou le DMP.

Dans ce cadre, la question du consentement du patient s'est alors posée et a été corrélée par le législateur à la notion d'équipe de soins, définie à l'article L 1110-12 du CSP : *« L'équipe de soins est un ensemble de professionnels qui participent directement au profit d'un même patient à la réalisation d'un acte diagnostique, thérapeutique, de compensation du handicap, de soulagement de la douleur ou de prévention de perte d'autonomie, ou aux actions nécessaires à la coordination de plusieurs de ces actes »* . L'équipe peut exercer dans le même établissement, peut être constituée par des professionnels concourant tous à la prise en charge du patient, ou dans une structure de soins où au moins un professionnel de santé exerce. Pour le partage des données médicales au sein de l'équipe de soin, le consentement est présumé, selon l'article L 1110-4 CPS. L'équipe peut alors échanger et partager les données du patient, dans le strict respect des règles réglementaires. Cela se comprend tout à fait au regard du besoin d'en connaître des différents médecins, infirmières, auxiliaires de santé intervenant dans la prise en charge du malade. Un diagnostic isolé, sans échange, est d'ailleurs souvent controversé.

En revanche, hors équipe de soin, l'article L 1110-4 III[72] dispose que « *le partage, entre des professionnels ne faisant pas partie de la même équipe de soins, d'informations nécessaires à la prise en charge d'une personne requiert son consentement préalable, recueilli par tout moyen, y compris de façon dématérialisée* ». Le législateur vise ici le consentement au sens de l'article 4 du RGPD, définissant le consentement au traitement des données à caractère personnel. Ainsi, le consentement n'est plus présumé, mais préalable à tout partage en dehors de l'équipe de soins ou entres équipes de soins distinctes. Il nécessite un recueil distinct de celui qui intervient à l'occasion de l'acte médical. Sur ce point, la CNIL exige un consentement libre, spécifique, univoque et éclairé, et écrit.

Comment comprendre ce changement de paradigme ? Il s'analyse au regard de l'enjeu de l'acceptation du patient à ce que ses données soient partagées, à d'autres professionnels de santé que ceux assurant habituellement sa prise en charge. Cela se lit également au travers de l'interopérabilité des systèmes d'information en santé. Cela fait référence à l'accès, l'intégration et l'utilisation des données de santé, entre personnes devant en connaitre, afin

[72]Création par le décret n° 2016-1349 du 10 octobre 2016

qu'elles puissent être utilisées pour optimiser les prises en charge des patients. François Macary (ASIP Santé, 2011) estime que c'est « *la capacité qu'ont plusieurs systèmes ou composantes d'échanger de l'information entre eux et d'utiliser l'information qui a été échangée* »[73]. In fine, cela permet aux soignants de recevoir, en temps quasi-réel et en toute sécurité, les données de santé d'un patient, d'un hôpital à un autre, au travers des outils informatiques de l'établissement.

Quelle a été la réponse du Droit face à un accès aux données de santé toujours plus large ? Quelle obligation repose sur les professionnels de santé ? Le respect du secret professionnel lors de l'échange et du partage des données de santé est la règle *(B).*

B) Un principe immuable : l'obligation de respecter le secret professionnel lors de l'échange et le partage des données de santé

«Il n'y a pas de médecine sans confiance, de confiance sans confidence et de confidence sans secret »

Professeur Louis Portes, Président du CNOM à l'académie des sciences morales et politiques, 5 juin 1950

Le traitement des données de santé est également encadré par l'obligation de secret pesant sur les professionnels de santé tel que défini à l'article L 1110-4 du Code de la santé publique, qui est, pour la Cour européenne des droits de l'homme, au cœur de la « *confiance des patients dans le corps médical et les services de santé en général* »[74]. Toute personne prise en charge par les services de santé a le droit au respect des informations la concernant. Ce secret professionnel, institué dans l'intérêt du malade, vaut particulièrement lors d'échange et de partage de données de santé. Le professionnel qui, à cette occasion, divulgue ces données sera sanctionné pénalement sur le visa de l'article 226-13 du Code pénal et encourt jusqu'à un an d'emprisonnement et 15 000 € d'amende.

L'évolution des pratiques, notamment les modes d'exercice coordonné en maisons de santé pluri professionnelles, en pôles de santé et en centres de santé, souligne la nécessité d'échanger et de partager entre professionnels de santé. Cela contribue également au décloisonnement Ville/Hôpital et à la promotion d'une prise en charge collaborative du patient, face aux défis que posent, entre autres, le vieillissement de la population et les

[73]Biedma, José María, et Christian Bourret. « Les enjeux des projets d'interopérabilité en santé pour la mobilité des citoyens. Le cas de l'Espagne », Projectics / Proyéctica / Projectique, vol. 13, no. 1, 2015, pp. 23-36.
[74] CEDH, 25 février 1997, Z. c/ Finlande, n°22009/93, pt.95

maladies chroniques. Plus encore, l'échange et le partage des données de santé a été décuplé depuis 2016, année de création des GHT par la loi MNSS. En effet, cette nouvelle organisation oblige les établissements partis à la convention constitutive du groupement à partager et communiquer davantage.

Au-delà des nouveaux modes d'exercice de la médecine, c'est la pandémie de Covid-19 qui a permis de re-questionner les contours du secret médical. L'article 1 du décret n° 2020-1690 du 25 décembre 2020[75] institue « *la création d'un traitement automatisé de données à caractère personnel dans le cadre de la campagne de vaccination contre la Covid-19, dénommé "Vaccin Covid"* ». Ainsi, l'ouverture par l'Assurance maladie de « Vaccin Covid » le 4 janvier 2021 a questionné. Sous la responsabilité de la CNAM et de la direction générale de la santé du Ministère des solidarités et de la santé, ce téléservice permet aux professionnels, dans le cadre de la lutte contre l'épidémie, d'avoir connaissance des données d'identification de la personne concernée et ses coordonnées, les données relatives à la réalisation de la vaccination (lieu de vaccination, type de vaccins, zone d'injection, date de sa réalisation etc.) et les données permettant d'identifier les professionnels de santé ayant réalisé chacune des étapes du cycle vaccinal. A première vue, l'utilisation d'un tel dispositif est louable, mais l'Assurance maladie précise que les données des vaccinés pourront être réutilisées et envoyées à une liste d'acteurs dont la longueur étonne : direction du numérique des ministères chargés des affaires sociales pour permettre l'information et l'orientation des personnes vaccinées en cas d'apparition d'un risque nouveau lié au vaccin ; service public d'information en santé, pour les seules informations relatives aux professionnels de santé et aux vaccinations possibles afin d'assurer sa mission de diffusion gratuite de l'offre de soins disponible auprès du grand public ; Santé publique France pour la mesure de l'efficacité vaccinale ; ARS pour assurer l'organisation de la campagne de vaccination à l'échelon régional et à son suivi ; direction de la recherche, des études, de l'évaluation et des statistiques (Drees) du ministère de la Santé, pour les données nécessaires à sa mission d'analyse et de diffusion des informations statistiques dans le domaine de la santé et enfin plateforme des données de santé et CNAM pour faciliter l'utilisation des données de santé pour les besoins

[75] Décret n° 2020-1690 du 25 décembre 2020 autorisant la création d'un traitement de données à caractère personnel relatif aux vaccinations contre la covid-19

de la gestion de l'urgence sanitaire et de l'amélioration des connaissances sur le virus, sauf opposition de la personne concernée. [76]

Le système d'informations « Vaccin Covid » avait fait l'objet d'une délibération de la CNIL[77] ; cette dernière s'était d'ailleurs montrée fébrile face au projet mais l'a validé pour autant. En effet, la Commission avait émis plusieurs remarques, la première relative au secret médical nous intéressant : « *seules les personnes habilitées et soumises au secret professionnel doivent pouvoir accéder aux données « Vaccin Covid », dans les strictes limites de leur besoin d'en connaître pour l'exercice de leurs missions.*
Il appartient donc au responsable de traitement de définir pour chaque destinataire des profils fonctionnels strictement limités aux besoins d'en connaitre pour l'exercice des missions des personnes habilitées. » A cela, la CNAM répondra que « *ce téléservice est exclusivement accessible aux professionnels de santé pour les données qui concernent les patients qu'ils prennent en charge.* » Lacunaire et vague, cette réponse n'apporte pas grande satisfaction, alors qu'il s'agit tout de même de la création d'un fichier de personnes vaccinées ou non contre la Covid 19, dont les informations de santé seront exploitées par les autorités publiques. Ainsi qu'elle conclut, la CNIL devra rester « vigilante » sur ce dispositif, qui deux ans après sa mise à disposition, n'a pas connu de cyberattaques ni de fuites de données.

Le respect du secret médical peut être mis à mal face à un échange et un partage des données de santé toujours plus important. La pratique démontre la difficulté qu'ont les professionnels à respecter le cadre dans la circulation de l'information. Une infirmière a pu me saisir de la question durant un de mes stages. Cette dernière a vu, sur le dossier patient informatisé d'un malade qu'il avait effectué un séjour en psychiatrie auparavant. Elle soulève, à juste titre, protection pour le patient, désormais hospitalisé pour des troubles somatiques, qui n'a certainement pas envie de dévoiler la totalité de ses antécédents médicaux, surtout si la prise en charge intervient longtemps après le séjour psychiatrique. Cela n'est pas réglé par les textes et une précision législative serait appréciable.

Parfois considéré comme contraignant, le consentement n'est pas toujours l'exception la plus adéquate pour traiter des données de santé. Surtout, la pratique médicale permet de s'en dispenser, car la prise en charge du patient légitime le traitement des données, protégées par le

[76] Vaccin Covid : un outil numérique pour le suivi de la vaccination, Ameli.fr, 4 mai 2022
[77] Délibération n° 2020-126 du 10 décembre 2020 portant avis sur un projet de décret autorisant la création d'un traitement de données à caractère personnel relatif à la gestion et au suivi des vaccinations contre le coronavirus SARS-CoV-2

secret médical. Cela justifie qu'il soit nécessaire de disposer d'autres exceptions que le consentement pour contourner le principe d'interdiction (Section II).

Section II : L'impérative nécessité de disposer d'exceptions autres que le consentement

Traiter les données de santé est une nécessité pour la santé publique et permet d'accélérer l'innovation pour améliorer les soins et les bénéfices patients ; dès lors que le risque de les compromettre est maitrisé. Dès lors, le RGPD et la LIL prévoient d'autres exceptions permettant de déroger au principe d'interdiction. L'on peut à nouveau s'interroger sur la pertinence du principe d'interdiction du traitement des données de santé, auquel l'on peut déroger si les intérêts vitaux d'une personne ou d'un tiers sont en jeu *(§1)* et si la personne elle-même, rend ses données de santé publiques *(§2).*

§1 : Le traitement des données de santé autorisé pour la sauvegarde des intérêts vitaux d'une personne physique

Cette exception, dont les contours peuvent être flous, mérite d'être explicitée (*A*). Elle a par ailleurs été sollicitée par les enjeux de la crise du Covid 19 *(B).*

A) Le contour de la notion de "sauvegarde des intérêts vitaux"

L'article 9.c du RGPD dispose que l'interdiction de traitement ne s'applique pas si *« le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique, dans le cas où la personne concernée se trouve dans l'incapacité physique ou juridique de donner son consentement »* .Le choix de traiter de cette exception m'est apparu nécessaire puisqu'elle mentionne l'incapacité de consentir, et se trouve donc relier à l'exception du consentement étudiée ci-dessus. La sauvegarde des intérêts vitaux se rapporte à la vie et à la santé humaine, et justifie, en pratique, qu'un établissement ou un professionnel de santé recueille des données sensibles dans une situation où la mort pèserait sur la personne ou un tiers. L'on comprend alors que cette exception justifie un traitement des données dans un contexte médical, puisqu'elle sera aussi utilisée lorsqu'une personne accidentée, dans un état grave est admise à l'hôpital inconsciente et dans l'incapacité de consentir au traitement de ses données de santé.

De plus, le considérant 46 du RGPD renforce cette exception, *« lorsque le traitement est nécessaire à des fins humanitaires, y compris pour suivre des épidémies et leur propagation, ou dans les cas d'urgence humanitaire, notamment les situations de catastrophe naturelle et d'origine humaine.* » Ce considérant fait explicitement référence à un contexte d'épidémie, et

l'actualité récente nous a fourni des exemples permettant de cerner si le Covid-19 pouvait être une menace contre les intérêts vitaux, légitimant alors des traitements de données de santé invasifs pour la vie privée.

Le RGPD a renforcé cette exception, en admettant que le traitement des données de santé est permis si les intérêts vitaux de toute autre personne sont en jeu ; il est encore nécessaire que la personne ne soit pas physiquement ou juridiquement capable de consentir, mais que l'on puisse présumer son consentement.

Durant la pandémie de Covid 19, la sauvegarde des intérêts vitaux a permis que l'on traite des données de santé, aux vues du contexte sanitaire et de la menace du virus sur la vie des populations (*B*)

B) Une exception utilisée durant la crise sanitaire du Covid 19

Les situations d'urgence sanitaires permettent de mettre en oeuvre des traitements de données de santé, que des situations de droit commun n'autoriseraient pas. A titre d'illustration, le décret du 12 mars 2020 est à l'origine de la mise en œuvre du fichier SIDEP par le ministère de la Santé et du fichier Contact covid par l'Assurance maladie.

Outre le traitement informatique de nos données de santé dans le cadre de la prévention et du dépistage du coronavirus, c'est bien la protection de cette collecte généralisée de données qui a pu inquiéter les citoyens. En effet, ces deux fichiers ont recueilli et traité des données de santé en très grand nombre, avec le concours de 600 laboratoires pharmaceutiques, de professionnels de santé à l'origine de la prescription des tests, des agences sanitaires et des organismes de sécurité sociale.

Pour le fichier Contact Covid, le décret du 12 mai 2020 liste les données concernées, qui sont notamment : *« d) la spécialité du médecin à l'origine de l'inscription dans le traitement de données » ; « g) les données relatives à la situation de la personne au moment du dépistage (hospitalisé, à domicile ou déjà à l'isolement) » ; « k) le cas échéant, la fréquentation, dans les quatorze derniers jours, des catégories d'établissements suivantes : établissement d'hébergement pour personnes âgées dépendantes, établissement médico-social, milieu scolaire, crèches, établissement de santé, établissement pénitentiaire ainsi que les coordonnées de l'établissement » ; « l) le cas échéant, la participation, dans les quatorze derniers jours, à un rassemblement de plus de dix personnes (localisation et date) »*

Une immixtion alors jamais constatée dans la vie privée des citoyens français, dont les habitudes de vie et de fréquentation de lieux sont livrées à l'Assurance maladie, responsable

du traitement du fichier Contact Covid. Le Ministère de la santé reste par ailleurs très vague quant à la protection des libertés individuelles, expliquant simplement que : « *Les garanties prévues par le règlement 2016/679 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 (RGPD) ont été appliquées aux traitements SI-DEP et "Contact Covid".* [78]

S'il est tentant de rapporter ce traitement de données de santé à l'intérêt vital, puisque le virus du Covid 19 compromet la vie des personnes, il n'en reste pas moins que cette exception n'est pas pleinement opérante. L'exception de l'intérêt public pour des motifs de santé publique laisse davantage de marge de manœuvre aux autorités, qui se servent alors de la base légale du même nom pour rendre le traitement des données licite.

A la lecture du RGPD, une autre exception peut étonner. Le texte aménage en effet, le contournement du principe d'interdiction du traitement des données de santé, si la personne rend elle-même publique ses informations (§2). Un sujet lourd de sens à l'aune de l'essor des réseaux sociaux.

§2 : La divulgation de ses données médicales par le patient lui-même : une exception difficile à appréhender

L'article 9.e du RGPD permet de contourner le principe d'interdiction si la personne rend elle-même ses données manifestement publiques ; exigeant alors un acte positif de publication de ses données *(A)*. Cette exception présente des enjeux à la fois éthiques et juridiques (*B*) car il s'agit de trouver un équilibre entre liberté d'expression des personnes et sécurité de leurs données de santé.

A) L'exigence d'une publication de données à l'initiative du patient

Cette exception au principe d'interdiction est celle qui pose en réalité, le plus de controverses. En effet, comment appréhender, au regard du droit, la divulgation par une personne de ses propres données médicales, par le biais des réseaux sociaux par exemple ? Le contrôle et par suite, la protection à apporter sur cette publicité est délicat puisque le patient lui-même fait le choix d'apporter à la connaissance de tous des informations sur sa santé, selon sa volonté.

[78] Ministère de la santé et de la prévention, 06/05/2020, « Contact-COVID et SI-DEP, les outils numériques du dépistage Covid-19

Logiquement, et parce que la publication de données de santé par la personne échappe au contrôle du médecin ou de l'hôpital dans le cas d'un dossier patient, le RGPD permet de déroger au principe d'interdiction lorsque *« le traitement porte sur des données à caractère personnel qui sont manifestement rendues publiques par la personne concernée »*.[79] Le texte ne donne pas davantage de précisions mais son interprétation permet de déduire que le traitement de données de santé devient admissible lorsqu'une personne les publie de manière évidente et intentionnelle, en toute conscience, sur une plateforme publique telle qu'un réseau social ou un forum en ligne. On entend alors que la personne a mis à disposition d'un groupe indéterminée, les informations les plus sensibles la concernant.

Cette exception interroge sur le plan juridique, car elle est la porte ouverte à de potentielles dérives, notamment la commercialisation des données de santé pourtant prohibées par le CSP[80] : « *Tout acte de cession à titre onéreux de données de santé identifiantes directement ou indirectement, y compris avec l'accord de la personne concernée, est interdit sous peine des sanctions prévues à l'article 226-21 du code pénal.* »

Un exemple nous est donné par le cas de la start-up française Embleema, qui a permis via une plateforme de santé, « *de faire le lien entre les chercheurs, demandeurs de données rares pour développer les traitements, et les patients capables de les générer. Cela permet aux patients de créer un carnet de santé virtuel, puis de le mettre à disposition des chercheurs via la blockchain, contre rémunération »*[81] Technologie de stockage et d'information, le blockchain permet à la société de voir quelle type de données est transportée sur la plateforme : *« un dossier médical, des données issues d'un objet connecté, ou des réponses à un questionnaire, mais sans en voir le détail. Les chercheurs intéressés par ces objets contactent la startup, définissent le type de données dont ils ont besoin avec une description précise de leur cible, et un budget. Après négociation du montant, la jeune pousse émet un contrat dans la blockchain avec la proposition de l'équipe de recherche. Un algorithme (validé par la Food and Drug Administration (FDA) américaine) détecte alors qui remplit les critères pour participer à l'étude et fait la proposition au patients concernés. Ces derniers disposent d'indications précises sur l'usage qui sera fait de ses données. S'ils acceptent, Embleema leur redistribuera une partie du montant du contrat. Pour trouver ces données, la startup signe des partenariats : elle travaille déjà avec l'institut de lutte contre le cancer*

[79] Article 9 paragraphe 2 point e
[80] Article L 1111-8 du Code de la santé publique
[81] François Mamens, " Embleema, la blockchain entre patients et chercheurs » La Tribune, 2019

Gustave-Roussy en France et avec une association de patients atteints de mucoviscidose aux Etats-Unis. »

Peut-on rattacher ce cas à l'exception de l'article 9-e du RGPD ? Oui, car c'est bien la personne qui met à disposition ses données sur la plateforme et les partage pour être revendues. Il y a donc une action positive du patient, qui permet à un tiers de traiter ses données de santé. Mais, en réalité, la plateforme agit dans la légalité car les données ne sont pas « à l'état brut » mais dénuées de toute information identifiante, ne permettant pas une identification de la personne. De plus, « *la technologie blockchain a pour rôle d'offrir des garanties de confidentialité, de traçabilité et de respect du consentement aux patients. Et surtout, elle lui redonne la main sur ses données, puisqu'elles ne sont pas mélangées avec celles d'autres patients par un tiers.* »

C'est en tout cas, un danger pour la vie privée, qui interroge sur les plans juridiques et éthiques *(B).*

B) Une exception à la croisée de problématiques juridiques et éthiques

L'exemple posé par le modèle économique de la société Embleema prouve que la santé est en plein bouleversement et se généralise aujourd'hui sur Internet ; elle « *connait depuis peu des changements manifestes en ce qui concerne la prise de pouvoir des patients sur leurs maladies ou celles de leurs proches. Internet a été un véritable catalyseur et a permis d'ouvrir de nombreux espaces virtuels (…) grâce auxquels les individus commentent et échangent quant à leurs pathologies. »*[82]. L'autopublication des données d'un patient échappe au contrôle du responsable de traitement que peut être l'hôpital ou le professionnel de santé. Il en va de la responsabilité individuelle. En revanche, le fait que le RGPD se saisisse de ce mésusage par la personne de ses données de santé pour admettre qu'elles puissent être traitées, interroge. Il aurait été plus opportun de ne pas consacrer cette possibilité dans le règlement, mais plutôt de la sanctionner et d'en prévenir les dérives.

La publication de ses données de santé par le patient lui-même peut être relié au développement d'Internet et des réseaux sociaux « de santé », sites généralistes (Doctissimo, fondé en 2000 par des médecins) ou consacrés à certaines pathologies en particulier.

[82]Menvielle, Loick, William Menvielle, et Anne-Francoise Audrain-Pontevia. « Effets de la fréquence d'utilisation des communautés virtuelles de patients sur la relation patients-médecins », Journal de gestion et d'économie médicales, vol. 34, no. 8, 2016, pp. 431-452.

Ainsi, j'ai souhaité consacrer un temps de mes recherches à la découverte du site Doctissimo, où j'ai pu accéder à un très grand nombre de données et d'informations médicales, directement publiées par les patients ou leurs proches ; dont la divulgation par un patient atteint de sclérose en plaque, de ses récents résultats médicaux. Cela pose question en termes de sécurité et de potentielle réutilisation. Mais, encore une fois, prédomine la volonté de la personne de porter à la connaissance de tous la pathologie dont elle souffre.

Le Conseil d'État a été saisi de cette exception dans un arrêt du 6 décembre 2019[83]. En l'espèce, une personne dont les données relatives à sa sexualité (classées au rang de données sensibles par l'article 9 du RGPD, tout comme les données de santé) avaient été publiées sur un site internet, en demande le déréférencement. Le Conseil d'état a considéré que le site pouvait légitimement les publier « *dès lors [qu'elles] sont issues du roman à caractère autobiographique* » de la personne concernée et qu'ainsi *« les données en cause doivent être regardées comme ayant été manifestement rendues publiques* ». Faisant ainsi écho à l'exception de l'article 9 point e du RGPD, les juges légitiment un tel traitement, en n'imposant pas au site de retenir une base légale cohérente avec cette exception. Les principes de sécurité juridique et de protection de la vie privée ont été bousculés par cette décision ; laissant penser que cette exception laisse place à l'interprétation des juges. En tout état de cause, la décision d'auto-publier ses données de santé peut nuire à la personne et pose une problématique éthique en termes de responsabilisation et d'usage de ces dernières.

Conclusion de la Partie I :

La transformation numérique du secteur de la santé s'accompagne nécessairement d'un cadre juridique, destiné à protéger la vie privée des personnes concernées par le traitement de leurs données de santé. L'Union européenne a doté ses états membres d'une ligne en suivre en matière de protection des données à caractère personnel, et cela s'est appliqué aux établissements sanitaires et médico-sociaux du territoire national ainsi qu'aux acteurs institutionnels de la santé. La loi de 1978 n'en est pas devenue obsolète et constitue encore un pilier de la protection des données. En revanche, modifiée et actualisée à de nombreuses reprises, elle a laissé au RGPD, une place de choix pour diriger la conformité du traitement des données de santé.

[83] Conseil d'Etat, 6 décembre 2019, n°409212

La collecte de ces données s'est imposée comme un enjeu de santé publique ces dernières années ; notamment en ce qu'elle permet de faire avancer la recherche médicale, mais aussi de permettre aux nouveaux modes d'exercice professionnel en santé de s'imposer (Télémédecine, exercice coordonné des professionnels du territoire par l'échange et le partage de données etc.). Le traitement fait de ces données doit s'exercer en conformité avec les règles législatives et réglementaires, dans l'intérêt d'un système de santé fournissant une sécurité suffisante à ses usagers. Une marge importante, consacrée par neuf exceptions est laissée aux acteurs de la santé, pour déroger au principe d'interdiction du traitement des données de santé. Le consentement du patient présente des limites et peut-être lui aussi, dépassé par d'autres exceptions, plus simples à mettre en œuvre pour les responsables de traitement.

En tout état de cause, le traitement des données de santé peut être générateur d'insécurité juridique et n'est pas exempt de risques ; qui ne sont pas sans poser de dilemmes éthiques. Le cadre juridique explicité ci-dessus, est complété par l'appréciation, l'interprétation et la protection des juridictions dans la mise en œuvre du traitement des données de santé (Partie II).

Partie II : Le traitement des données de santé, dilemmes éthiques et protection par le Droit

L'éthique est rapportée à plusieurs définitions, forgée au fil du temps par la philosophie de Kant ou de Ricoeur, qui énonçait l'éthique comme « *tout le questionnement qui précède l'introduction de l'idée de la loi morale* »[84]. Il convient de retenir que l'éthique fonde « *l'ensemble des principes moraux à la base de la conduite de quelqu'un* » selon le dictionnaire Larousse. Mais, l'éthique médicale est à distinguer de l'éthique du numérique en santé. Les dimensions de l'éthique médicale sont soutenues par les principes fondateurs d'Hippocrate : la Justice, l'Autonomie, la Bienfaisance et la Non-malfaisance. En revanche, sur l'éthique appliquée au numérique en santé, l'ANS relève d'autres principes que sont l'intégrité des données, la confidentialité des données, la compréhension des patients, le contrôle du consentement par les patients, le respect de l'autonomie décisionnelle, l'explicabilité des systèmes, le maintien d'une relation humanisé (empathie), etc.

L'éthique n'est pas le droit, elle est le fruit d'un questionnement sur les valeurs et principes moraux à développer, pour une utilisation respectueuse et pérenne du numérique en santé, toujours dans une logique de responsabilisation des acteurs. (Chapitre I). Le temps de la responsabilité, sanctionnée par des normes écrites, vient lors de la protection des données de santé par les autorités régulatrices et les organes juridictionnels (Chapitre II*)*

Chapitre I : L'éthique dans le traitement des données de santé

Le Comité Consultatif National d'Éthique (CCNE) dans un avis du 29 mai 2019 a mis en lumière que *«trois principes éthiques peuvent être fragilisés par l'utilisation des données massives : le secret médical, par la multiplication des informations partagées et échangées entre divers acteurs, dont certains ne relèvent pas du milieu médical ; la responsabilité de la décision médicale, par le risque d'automatisation que crée la multiplication des logiciels algorithmiques; la relation personnelle entre le médecin et son patient, qui est menacée d'appauvrissement avec les innovations attendues du traitement des données massives, le patient risquant d'être réduit à un ensemble de données à interpréter, semblant rendre inutile son écoute.* » [85]

[84]Ricoeur P. ; Fondements de l'éthique, dans Autres Temps, 1984, pp. 61-7

[85] Données massives et santé : une nouvelle approche des enjeux éthiques, CCNE, Avis rendu public le 29 mai 2019 page 8

Face à ce constat, il est impératif de laisser au patient, au stade de sa prise en charge hospitalière, une marge d'action dans le traitement de ses données de santé (Section I). Le besoin d'éthique se verra renforcé lorsque le traitement des données de santé intervient dans le cadre de recherches médicales (Section II).

Section I : La maitrise laissée au patient dans le traitement de ses données de santé

Le patient a-t-il véritablement le choix ? Pour avoir le choix, il faut être libre et sans contrainte. Ce n'est pas le cas dans le cadre du traitement des données de santé ; s'y opposer formellement contreviendrait à la bonne prise en charge médicale de la personne, à la circulation de ses informations médico-administratives, à son parcours de soins et ses remboursements.

Mais, au même titre que dans son parcours de soin, les pouvoirs publics souhaitent laisser au patient la maitrise de ses choix et en l'occurrence ici, de ses données personnelles. Cela passe par une obligation d'information envers le patient (§1) concernant l'utilisation faite de ses données ; afin qu'il exerce pleinement les droits qui lui sont octroyés par le corpus juridique (§2).

§1 : L'obligation d'information dévolue au patient, garantie d'un consentement libre, spécifique et éclairé et univoque

Le consentement au traitement des données de santé du patient, pour être en adéquation avec le respect de sa privée et de son autonomie de décision, doit être obtenu après la délivrance d'une information appropriée (*A*). Le sens même de cette information est pour le patient, la sauvegarde de l'autonomie de sa volonté (*B*).

A) Le contenu de l'information : informer le patient sur l'usage du numérique en santé

Obligation déontologique et légale, le devoir d'information du médecin est plus connu sous l'angle de l'acte médical. A ce titre, l'article 35 du Code de déontologie médicale dispose : « *Le médecin doit à la personne qu'il examine, qu'il soigne ou qu'il conseille, une information loyale, claire et appropriée sur son état, les investigations et les soins qu'il lui propose. Tout au long de la maladie, il tient compte de la personnalité du patient dans ses explications et veille à leur compréhension.* ». L'article L 1111-2 du CSP rappelle lui, que : *« Toute personne a le droit d'être informée sur son état de santé ».* Ces textes étant propre à l'information médicale, ils ne fondent pas l'information due au patient à l'occasion du traitement de ses

données de santé. Ainsi, il convient de se rapporter au RGPD, qui impose une « *information concise, transparente, compréhensible et aisément accessible des personnes concernées* »[86], ainsi qu'à la LIL, qui avait déjà prévu l'information de la personne concernée à l'article 116 I.

A l'hôpital, les principales informations délivrées au patient sont la finalité du traitement de ses données de santé et sa base légale, leur durée de conservation, l'identité du responsable de traitement et du DPD, les destinataires des données, les intérêts légitimes poursuivis par le responsable du traitement ou par un tiers et le transfert des données s'il intervient. En réalité, l'enjeu éthique ici est de lier l'information sur l'utilisation des données de santé avec la connaissance du numérique en santé. La circonstance pour un patient de s'opposer au traitement de ses données de santé sera réduite si celui-ci est au fait des bénéfices apportés par le numérique dans son parcours de soins. Plus important encore, l'information doit porter sur les droits accordés par le RGPD à la personne dont les données sont traitées, au cœur de la confiance des citoyens dans le numérique en santé.[87]

Qu'en est-il de l'information dévolue par l'État, lorsqu'il met à disposition des personnes, les outils de l'e-santé ? Dans le cas du DMP, la CNIL a précisé qu'il incombait à l'État d'informer les usagers de ces outils sur leurs droits, faute de quoi, il ne serait pas en conformité avec le RGPD[88]. Depuis janvier 2022, l'Espace Numérique de Santé (ENS) a intégré le DMP et une nouvelle information est due aux assurés sociaux. La CNIL précise que « *la délivrance de l'information est prévue par des moyens multiples : sur le site web dédié de l'Assurance maladie, via des brochures ou encore des campagnes d'information* ». En tout état de cause, une information préalable est prévue, mais le consentement des personnes n'est pas requis. Le mécanisme de l'opt-out[89], qui permet de s'en dispenser été retenu pour la création de l'ENS. Cela fera l'objet de développements ci-dessous.

Sur le plan éthique, l'obligation d'informer le patient sur le traitement de ses données permet de sauvegarder l'autonomie de sa volonté (*B*).

---

[86]Articles 12, 13, 14 du RGPD

[87] Confer. Paragraphe 2 ci-dessous

[88] Délibération n° 2021-050 du 15 avril 2021 portant avis sur un projet de décret relatif au dossier médical partagé (demande d'avis n° 21001149)

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

B) Le sens de l'information : la sauvegarde de l'autonomie de la volonté du patient

Le traitement des données de santé fait face à l'éthique médicale, dont un des grands principes contenus dans le Serment d'Hippocrate est l'autonomie. Les patients et les professionnels de santé doivent conserver leur autonomie de pensée, d'intention et d'action lorsqu'ils prennent des décisions. Alors, dans un monde où le numérique en santé prend un tournant de plus en plus pressant voire envahissant, comment les patients les moins susceptibles de s'y adapter font-ils pour consentir librement ? Sont-ils vraiment décisionnaires ?

Afin de répondre à ces questions, la Délégation ministérielle au Numérique en Santé du ministère de la Santé et des Solidarités s'est dotée d'une cellule Éthique. Elle pour mission de faire de l'éthique un élément central du virage numérique en santé, notamment grâce à l'élaboration d'outils pratiques de sensibilisation, d'évaluation et de labellisation à destination des professionnels de santé, des industriels, des usagers du système de santé et des pouvoirs publics. Dans le cadre de ce mémoire, j'ai pu m'entretenir avec deux juristes de la DNS, Madame Passemard et Monsieur Duret. Je les ai questionnés sur le regard porté au consentement du patient au traitement de ses données de santé. Selon eux, le véritable enjeu pour les professionnels est d'informer clairement le patient et recueillir son consentement éclairé pour le partage des données hors équipe de soins. Il est d'intérêt général de laisser son libre arbitre au patient et de ne pas rentrer dans une ère de contrôle des données de santé. La DNS élabore des modèles types de recueil de consentement, en collaboration avec l'ANS afin d'aider les professionnels de la santé.

La numérisation de la santé se heurte, en plus d'un devoir d'information accru, à la fracture numérique. J'ai donc interpellé la DNS sur les difficultés d'accès aux technologies de communication de certaines personnes pour des raisons soit de mauvaise couverture géographique, soit de conditions socio-économiques défavorables (fracture numérique). Comment, dans ces conditions, assurer un égal accès pour tous aux innovations dans le domaine de la santé et à l'information ? Le citoyen a été placé au cœur du développement de la santé numérique, avec la mise en place par la DNS et l'ANS, d'un Comité citoyen. Cela a permis de débattre et mettre en exergue les populations touchées par la fracture numérique : personnes âgées, français des DOM-TOM, citoyens les plus précaires, habitants de zone blanche. Afin d'agir pour les 13 millions de français dans cette situation et afin d'opérer un lancement réussi pour l'Espace Santé Numérique, la DNS a mis en place un programme d'accompagnement des citoyens pour la prise en main de Mon espace santé. Elle finance ainsi dix-huit postes de coordinateur régional des « ambassadeurs Mon espace santé ». Elle réalise,

avec l'ANS, un Tour de France de l'e-santé, dont la première étape a été réalisée aux Hôpitaux Universitaires Henri-Mondor. La DNS espère ainsi promouvoir une inclusion numérique et un accès simplifié à l'e-santé pour tous et permettre aux personnes de conserver leur autonomie face à la numérisation de la santé.

L'information préalable au traitement des données de santé, permet dans un second temps, l'exercice de droits par la personne qui en fait l'objet (§2).

§ 2 : Un axe cardinal du traitement des données de santé : les droits de la personne concernée

La numérisation de la santé produit une facilitation certaine du traitement des données de santé. Mais la simplification et la rapidité ne doivent pas dépourvoir les patients des droits sur leurs données de santé, octroyés par le législateur. Depuis 2018, le RGPD a renforcé les droits des personnes concernées par le traitement de leurs données personnelles (*B*). Parmi ces derniers, le droit d'opposition mérite une attention particulière (*A*).

A) Le droit d'opposition : un droit en tension

S'opposer au traitement de ses données à caractère personnel signifie en refuser l'utilisation, lorsque des raisons spécifiques le justifient. Deux dispositions importantes régissent le droit d'opposition : l'article L 1110-4 du CSP " *La personne est dûment informée de son droit d'exercer une opposition à l'échange et au partage d'informations la concernant. Elle peut exercer ce droit à tout moment* " et l'article 21 du RGPD : « *La personne concernée a le droit de s'opposer à tout moment, pour des raisons tenant à sa situation particulière, à un traitement des données à caractère personnel la concernant (…)* »

Après avoir démontré que les intérêts de la santé justifient un traitement des données de santé quasi systématique, notamment pour la prise en charge sanitaire du patient ou pour les besoins de la recherche ou de la santé publique, il s'agit de souligner des cas où le droit d'opposition va pouvoir être accordé au patient pour contrebalancer cette vérité. A l'hôpital, si le patient refuse de communiquer ses informations de santé, cela contreviendra nécessairement à ses soins. De ce fait, le mécanisme du consentement présumé au traitement des données de santé prime, sauf cas particuliers.

De plus, le droit d'opposition n'est pas un droit absolu. Le responsable de traitement peut continuer à traiter les données, « *s'il démontre qu'il existe des motifs légitimes et impérieux pour le traitement qui prévalent sur les intérêts et les droits et libertés de la personne*

concernée (...) »[90] Le cas contraire, il est de sa responsabilité de cesser sans délai le traitement de la donnée. Avant le RGPD, en vertu de l'article 38 de la loi du 6 janvier 1978, c'était à la personne de démontrer l'intérêt légitime pour que son droit d'opposition lui soit octroyé. On constatait donc une faiblesse, une lacune dans cette potentielle opposition. Désormais, c'est au responsable de traitement d'apporter un motif légitime pour continuer à traiter les données de santé de la personne : malgré un renforcement du droit d'opposition, l'article 21 du RGPD lui appose encore une restriction.

A l'hôpital, le cas le plus fréquent d'opposition est l'utilisation, pour la recherche, les études et l'évaluation des données de santé. En revanche, dans le cadre des soins, le patient se verra refuser son droit d'opposition, sur le motif légitime de l'obligation légale (formalisation du dossier médical, recueil des données médico-administratives pour les organismes sociaux, facturation…). Force est de constater un affaiblissement de ce droit d'opposition strict, au profit du mécanisme de l' « opt-out » prévu par la loi OTSS de 2019. Il permet à la personne de se désengager lorsqu'un traitement de ses données personnelles a été créé sur la base d'un consentement par défaut. Ce mécanisme a été retenu pour l'ouverture de l'Espace Numérique de Santé de chaque citoyen français, avec la possibilité pour l'usager de refuser la création de son dossier. Mais, s'il ne s'oppose pas, le dossier est créé avec un consentement par défaut. L'opposition intervient donc a posteriori.

L'étude de ce premier droit permet de constater qu'il est frappé d'incertitudes, et que la maitrise du patient sur ses données de santé n'est que relative. D'autres droits sont accordés, renforcés par le RGPD, mais nous verrons qu'ils ne sont pas systématiquement ni inconditionnellement applicables (*B*).

B) Des droits subsidiaires permettant au patient de garder la maîtrise de ses données

Les droits de la personne concernée par le traitement de ses données de santé ont été renforcés avec l'arrivée du RGPD. On compte le droit d'opposition explicité ci-dessus, le droit d'information (articles 12,13,14), le droit d'accès (article 15), le droit à la limitation des données (article 18), le droit à l'effacement (article 17), le droit à la rectification (article 16), le droit à la portabilité (article 20) Si nul n'est censé ignorer la loi, cet adage est en réalité impossible à appliquer dans la pratique médicale, ni dans le parcours de soins du patient. Voyons-nous chaque usager du système de santé consulter cumulativement le Code de santé

[90] Article 21 RGPD

publique, le RGPD et la loi Informatiques et Libertés avant de se rendre dans un lieu de soin et afin de connaitre ses droits en matière de traitement de ses données de santé ? Cela parait invraisemblable. Pourtant, de la part des acteurs du numérique en santé, le mot d'ordre est de "*rendre aux citoyens le contrôle de leurs données personnelles"* selon Cécile Courrèges, ex-directrice de la DGOS. Encore une fois, la pratique en établissement est différente. La responsabilité d'informer le patient sur ses droits revient alors au responsable de traitement des données : le directeur, souvent par l'intermédiaire du DPD.

Depuis l'entrée en vigueur du RGPD, les établissements de santé sont dans l'obligation de renseigner les patients sur la gestion de leurs données de santé, et les droits s'y rattachant. Le livret d'accueil, destiné dans un premier temps à informer le patient sur les missions de l'établissement, son séjour, les formalités administratives, a vu son rôle renforcé depuis 2018. Il peut désormais contenir les droits consacrés par le RGPD, ainsi que l'information dévolue au patient sur le traitement de ses données. Mais, force fut de constater au cours de mon stage à la Polyclinique St Laurent, que le livret d'accueil est peu ou pas consulté par les patients et qu'ils ne s'informent pas sur le traitement de leurs données de santé. Ainsi, sur douze patients, plus de la moitié ne connaissaient pas leurs droits en matière de protection des données à caractère personnel et n'avait pas lu la partie RGPD du livret d'accueil[91]. En revanche, beaucoup se sont interrogés sur l'utilité de la conservation de leurs données et sur les personnes ayant accès à ces informations ; prenant ainsi l'ampleur des enjeux du traitement des données de santé. Il s'agit donc désormais pour les responsables de traitement de poursuivre leur mission d'information et d'accompagnement des usagers au droit des données de santé ; avec pour ligne directrice : la confiance. Cela passe par des garanties solides de protection la vie privée des personnes (*Section II)*, notamment lorsque la recherche médicale intervient.

[91] Annexe 2

Section II : Un besoin renforcé d'éthique dans le domaine de la recherche médicale

Point 7 de la Déclaration d'Helsinki de l'Association Médicale Mondiale : « La recherche médicale est soumise à des normes éthiques qui promeuvent et assurent le respect de tous les êtres humains et qui protègent leur santé et leurs droits. »

La recherche médicale connait une structuration et une organisation évolutive depuis que l'ordonnance du 30 décembre 1958[92] a créé les Centres Hospitaliers Universitaires (CHU), et a par la même occasion, fondé l'ère moderne de la recherche médicale. La Déclaration d'Helsinki de 1964[93] impose pour les promoteurs et investigateurs des considérations éthiques, comme la protection de la vie privée et le respect de l'intimité des personnes se prêtant à la recherche, qu'elle implique ou non la personne humaine.

La présente section se concentrera d'ailleurs sur les Recherches Impliquant la Personne Humaine (RIPH). La loi du 5 mars 2012 dite Jardé[94], modifiée en 2016 et précisée en 2018, est le cadre juridique de référence pour les recherches médicales. Elle régit les RIPH en droit français, définies comme « *les recherches organisées et pratiquées sur l'être humain en vue du développement des connaissances biologiques ou médicale* » selon l'article L 1121-1 du CSP et en distingue trois types :

- Type 1 : les recherches interventionnelles comportant une intervention non dénuée de risque sur les participants.
- Type 2 : Les recherches interventionnelles comportant des risques et des contraintes minimes pour les participants.
- Type 3 : Les recherches non interventionnelles qui sont des recherches impliquant la personne humaine, mais qui ne comportent aucun risque ni contrainte et dans lesquelles tous les actes sont pratiqués de manière habituelle.

La recherche impose de hauts besoins d'éthique, guidés par le nécessaire respect de la vie privée et de l'intégrité corporelle des personnes. Par exemple, des exigences propres à la protection des données de santé s'appliquent dans ce cadre.

---

[92] 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

[93] Déclaration d'Helsinki de l'Association médicale mondiale ; Principes éthiques applicables aux recherches médicales sur des sujets humains. Adoptée par la 18e Assemblée générale, Helsinki, Juin 1964

[94] Loi n° 2012-300 du 5 mars 2012 relative aux recherches impliquant la personne humaine

Ces exigences ont trouvé pour solution des procédés techniques permettant de réutiliser les données de santé (§1), renforcée par un encadrement juridique supplémentaire (§2).

§1 : La réutilisation des données de santé dans les recherches impliquant la personne humaine

« Les données personnelles de santé sont un enjeu de premier plan pour la recherche dans le domaine de la santé. Elles sont le matériau de recherche de base pour les scientifiques (…) C'est pourquoi leur exploitation représente une opportunité de première importance »[95] pour le patient individuellement et pour la collectivité. La recherche médicale n'échappe pas au besoin constant d'éthique dans le traitement des données de santé. La réutilisation des données de santé pose une première problématique, qu'est l'éventuelle réidentification de la personne *(A),* à laquelle la législation sur les entrepôts de données de santé tente d'apporter solution (*B*).

A) Le problème éthique : l'éventuelle réidentification de la personne, forces et faiblesses de l'anonymisation

« Le droit au respect de la vie privée est sans conteste conçu comme une obstruction dans les avancées de la recherche médicale. Pourtant cette dernière doit se construire dans le respect des droits de l'Homme » [96]Ainsi, dans le domaine de la recherche médicale, qu'elle soit interne à l'hôpital ou multicentrique, les données de santé collectées à l'occasion de la prise en charge primaire, constituent une ressource essentielle pour les chercheurs, pour l'innovation, mais également pour les services de l'État dans la lutte contre les menaces sanitaires ou en matière d'épidémiologie.

Dans l'objectif, toujours prégnant en matière de données personnelles, de garantir la vie privée des personnes, l'anonymisation s'est imposée comme une solution à toute recherche médicale. Elle « *consiste à masquer les informations personnelles présentes dans les documents tout en préservant les informations cliniques* »[97]. Initialement, la ré-exploitation des données personnelles est interdite, mais l'anonymisation permet de contrer cela, en ouvrant des potentiels de réutilisation et en garantissant, théoriquement, la vie privée des

[95]LESAULNIER F., Recherche en santé et protection des données personnelles à l'heure du RGPD, In NETTER (E.), Regards sur le nouveau droit des données personnelles, Ceprisca, 2019, p. 303.
[96]GAMBARDELLA S., Une lecture de la jurisprudence de la Cour européenne des droits de l'Homme relative aux données de santé, Revue de droit sanitaire et social, Sirey, Dalloz, 2016.
[97]GROUIN C. ; Anonymisation de documents cliniques : performances et limites des méthodes symboliques et par apprentissage statistique. Bio-informatique [q-bio.QM]. Université Pierre et Marie Curie - Paris VI, 2013.

personnes. En revanche, la technique a ses faiblesses, conduisant le G29 à déduire que : « *les responsables du traitement des données devraient être conscients qu'un ensemble de données anonymisées peut encore présenter des risques résiduels pour les personnes concernées. »* [98]

De plus, la loi est très claire sur ce point ; rares sont les cas où elle impose un anonymat total des personnes. Cela ne concerne que la prise en charge des toxicomanes volontaires pour une cure de désintoxication[99], les activités de prévention, de dépistage, de diagnostic et de traitement ambulatoire des infections sexuellement transmissibles[100], l'accouchement sous X[101] et l'interruption volontaire de grossesses des mineures[102]

En sus de cette considération, il convient de souligner que la protection des données personnelles n'est plus assurée lorsque ces dernières sont rendues anonymes. En effet, le RGPD mentionne l'anonymisation au considérant 26, et ce afin d'exclure les données anonymisées du champ d'application de la législation relative à la protection des données :*« Il n'y a dès lors pas lieu d'appliquer les principes relatifs à la protection des données aux informations anonymes, (…) ni aux données à caractère personnel rendues anonymes de telle manière que la personne concernée ne soit pas ou plus identifiable »* En effet, la réutilisation des données anonymisées n'a pas d'impact sur la vie privée des personnes. En revanche, cela reste un traitement de données de santé, et les droits de la personne perdurent ; surtout celui d'être informée et de consentir ou a minima, de s'opposer.

On constate donc que l'anonymisation, car elle ouvre une possibilité de ré-identifier la personne, n'est pas exempte de défauts et ne permet pas de remplir totalement les exigences du RGPD ni celles de l'article 24 de la Déclaration d'Helsinki, disposant que *« toutes les précautions doivent être prises pour protéger la vie privée et la confidentialité des informations personnelles concernant les personnes impliquées dans la recherche. »*

Dès lors, la sécurisation des données de santé des personnes se prêtant à la recherche médicale exigence des garanties supplémentaires *(B).*

[98] Groupe de travail « article 29 » sur la protection des données, Avis 05/2014 sur les Techniques d'anonymisation, 0829/14/FR, 10 avril 2014
[99] Article R. 1112-38 du Code de la santé publique
[100] Article L. 3121-2-1 du Code de la santé publique
[101] Articles R. 1112-28 du Code de la santé publique et 326 du Code civil
[102] Article L. 132-1 du Code de la sécurité sociale

B) L'exigence de protection suffisante des données de santé : pari réussi du Système National des Données de Santé ?

Le développement ci-dessus met en exergue les limites de l'anonymisation du point de vue de la sécurisation des données. Dès lors, pour certains traitements de données de santé, particulièrement sensibles en raison de leur volume, la pseudonymisation a été retenue.

L'article 4.5 du RGPD la définit comme « le *traitement de données à caractère personnel de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, (…) afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable».* Ainsi, les données des personnes sont remplacées par un pseudonyme, c'est-à-dire un code ne permettant pas de rattacher l'individu à une identité.

Un tel mécanisme a été mis en œuvre par le SNDS, qui comporte les données relatives aux hospitalisations, aux consommations de soins ambulatoires, ainsi que les données sur les décès et leur motif de l'ensemble des Français, ainsi que l'exige l'article R1461-7 du CSP.

Par sa richesse et son exhaustivité, l'exploitation du SNDS a permis de répondre à des questions de santé publique. On comprend donc qu'au regard des besoins de l'avancée de la recherche médicale, la réutilisation des données de santé est un impératif et que la pseudonymisation des données répond aux enjeux de la recherche et l'innovation.

Historiquement, l'une des premières études sur les données du SNDS a démontré la mise en cause du Médiator dans la survenue de valvulopathies cardiaques. Plus récemment, cette base a permis d'identifier et de quantifier la nocivité pour le fœtus de la Dépakine prise par les femmes enceintes[103], ou de souligner le lien entre vaccin contre le cancer du col de l'utérus (anti-HPV) et maladie auto-inflammatoire chez les jeunes filles.

L'utilisation de données pseudonymisées au sein du SNDS répond donc à un double objectif :

- Le besoin d'une éthique renforcée dans la réutilisation des données de santé, afin de concilier vie privée et le besoin d'en connaitre afin d'accélérer la recherche et l'innovation en santé.
- Les exigences de la législation sur la protection des données personnelles, en matière de sécurité et de traçabilité des données.

[103] Le Monde, « L'enjeu crucial des données de santé », 3 février 2022 https://www.lemonde.fr/idees/article/2022/02/03/l-enjeu-crucial-des-donnees-de-sante_6112125_3232.html

L'absence de réidentification des personnes ne suffit pas toujours à permettre la recherche médicale. Un encadrement juridique supplémentaire est instauré et contribue à la bonne conduite des recherches médicales. (§2)

§2 : L'encadrement juridique supplémentaire nécessaire à une éthique des données renforcée des recherches impliquant la personne

La loi Jardé accroit le travail des Comités de protection des personnes (CPP), chargés d'émettre un avis conforme préalablement à toute recherche médicale. Leur rôle, visant entre autres, à garantir l'éthique des données utilisées pour les RIPH *(A)*, est majeur et se complète avec celui de la CNIL, chargée d'établir des méthodologies de références *(B)* pour protéger les données personnelles dans le cadre de la recherche médicale.

A) Le rôle des Comités de protection des personnes

Les CPP ont en charge l'évaluation de l'éthique dans les RIPH. Ils ont été créés par la loi du 9 aout 2004[104] relative à la politique de santé publique, et remplacent les Comités Consultatifs de Protection des Personnes dans la Recherche Biomédicale (CCPPRB) créés par la loi du 20 décembre 1988[105]. Leurs membres sont nommés par le directeur général de l'ARS, dans la région où le comité a son siège. Les CPP regroupent des personnes issues de cinq disciplines différentes : biomédical, éthique, sociologie, psychologie et juridique

Les trois types de recherches nécessitent toutes un avis conforme du CPP. Outre le respect de la protection corporelle, de l'intégrité, du consentement des personnes se prêtant à la recherche, l'article L 1123-7 du CSP attribue aux différents CPP des compétences précises en matière de protection des données à caractère personnel. Ce dernier dispose que : « *Le comité rend son avis sur les conditions de validité de la recherche, notamment au regard de (...) la méthodologie de la recherche au regard des dispositions de la loi n° 78-17 du 6 janvier 1978 , la nécessité du recours à la collecte et au traitement de données à caractère personnel et la pertinence de celles-ci par rapport à l'objectif de la recherche, préalablement à la saisine de la Commission nationale de l'informatique et des libertés.* » Ainsi, les CPP disposent, en plus d'une expertise scientifique, d'une expertise technique leur permettant de se prononcer sur le bien-fondé et le respect du traitement de données personnelles des personnes se prêtant à la recherche médicale. La réutilisation des données de santé dans la recherche nécessitant un consentement écrit, ou à minima une non-opposition, les CPP auront

[104] Loi n° 2004-806 du 9 août 2004 relative à la politique de santé publique
[105] Loi n° 88-1138 du 20 décembre 1988 relative à la protection des personnes qui se prêtent à des recherches biomédicales

notamment la tache de vérifier cela. Le cadre légal et réglementaire impose aujourd'hui à ces comités de vérifier la conformité au RGPD du traitement de données intervenant à l'occasion d'une RIPH. Le document de référence leur permettant de formuler un avis motivé, est la notice d'information RGPD fournie aux participants à la recherche par le promoteur, c'est-à-dire à la personne physique ou la personne morale qui est responsable d'une recherche impliquant la personne humaine, qui en assure la gestion et vérifie que son financement est prévu[106]. Le CSP impose ce document, fixant à la fois le cadre et l'objectif de la recherche, mais rappelant également la nécessité d'un traitement de données personnelles pour la mener à bien.

Ainsi, les CPP ne se substituent pas à la CNIL ; et ne contrôlent pas le respect de la base légale prévue pour la recherche médicale, ni l'exception utilisée pour traiter les données. Leurs rôles sont donc complémentaires, la CNIL intervenant seulement après avis d'un CPP sur la recherche, qui se doit d'être conforme à une méthodologie de référence. *(B)*

B) Les méthodologies de référence (MR)

La demande d'autorisation de la CNIL pour le traitement de données personnelles dans le cadre des RIPH est devenue exceptionnelle, au profit de l'obligation pour le promoteur de la recherche de se conformer à une méthodologie de référence. Elles sont l'œuvre de la CNIL, autorisée à publier des MR en vertu de l'article 11 de la LIL, et permettent au promoteur de respecter les règles légales et réglementaires relatives à la protection des données personnelles. Adoptées par délibération de la Commission, elles permettent à une étude de rentrer dans un cadre, la dispensant d'autorisation. Cela représente un gain de temps considérable pour les chercheurs et les hôpitaux.

Les six MR de la CNIL ne concernent pas toutes les RIPH. Seules les trois premières sont à soulever : **la MR-001** relative aux traitements de données à caractère personnel mis en œuvre dans le cadre des recherches dans le domaine de la santé nécessitant le recueil du consentement de la personne concernée; **la MR-002** relative aux traitements de données à caractère personnel mis en œuvre dans le cadre des études non interventionnelles de performances en matière de dispositifs médicaux de diagnostic in vitro; et **la MR-003** relative aux traitements de données à caractère personnel mis en œuvre dans le cadre des

[106] Article L 1121-1 du Code de la santé publique

recherches dans le domaine de la santé ne nécessitant pas le recueil du consentement de la personne concernée

Les MR permettent d'appuyer la culture de responsabilisation qui pèse désormais sur les acteurs de la santé, et particulièrement sur les responsables de traitement de données de santé. Dans le cadre d'une RIPH, la MR permet au promoteur d'identifier seul si son étude rentre dans le cadre d'objectifs et de finalités autorisés par le RGPD, la durée de conservation qu'il devra mettre en œuvre, mais aussi les données qu'il est autorisé à collecter et au moyen de quel type de recueil de consentement auprès du patient. La CNIL, par la simplification du régime d'autorisation du traitement des données personnelles, contribue à l'accélération de la recherche médicale et de l'innovation, tout en permettant de conserver un cadre éthique au stade de la réutilisation des dites données.

Le présent chapitre aura donc permis de démontrer que l'éthique médicale ne se limite pas aux principes généraux de la médecine d'Hippocrate, mais s'est adaptée aux évolutions du numérique en santé. J'ai cherché à souligner que le défi de l'information, et par suite du consentement de la personne, est majeur pour l'éthique dans le traitement des données de santé. Débiteurs de l'information, les patients sont acteurs du traitement de leurs données de santé, à condition d'en saisir les enjeux. Leurs droits sont en proie à d'importantes évolutions, notamment au regard des besoins de la recherche médicale dont la réutilisation des données de santé est une condition de son succès.

Le droit des données de santé ne saurait se satisfaire d'une approche éthique, qui ne peut à elle seule, contenir les dérives potentielles du traitement des données. Ainsi, le chapitre 2 abordera la protection des données de santé, sous l'angle du droit français et de l'Union Européenne. La protection passe par la régulation, qui relève de l'office de la CNIL.

Chapitre II : La protection des données de santé par les autorités régulatrices et les organes juridictionnels

Article 8-1 de la Charte européenne des droits fondamentaux : Toute personne a droit à la protection des données à caractère personnel la concernant.

Selon les chiffres de la CNIL, une multiplication par 3 des violations de données liées à des attaques informatiques sur des établissements de santé (centre hospitalier, clinique, EPHAD, maison de santé, établissements de soin, laboratoires etc.) a été constatée (12 violations en 2019 et 36 violations en 2020).

Ainsi, dans quelle mesure les tribunaux permettent-il d'offrir des garanties suffisantes de protection des données de santé ? Le droit, face à l'open data, suffit-il à encadrer le traitement des données de santé ? La CNIL (Section I) a une position, que je nommerai « régulatrice » envers le droit des données de santé. Le contrôle des juridictions nationales et européennes garantit, quant à lui, le respect de la balance entre traitement des données de santé et impératifs de respect de la vie privée et de confidentialité (Section II).

Section I : La régulation des données de santé par la CNIL

La protection des données de santé passe en premier lieu, par le contrôle de la CNIL, autorité administrative indépendante, créée par la LIL de 1978, qui surprend par l'ambivalence de son rôle (§1) et par l'influence positive du droit mou qu'elle édicte (§2).

§1 : La CNIL, autorité au rôle ambivalent

L'ambivalence du rôle de la CNIL se traduit à plusieurs égards. Elle est la première conseillère du gouvernement en matière de traitement des données de santé. Elle est à mon sens, le rempart contre le traitement frauduleux des données de santé. Avant d'avoir un rôle sanctionnateur, la CNIL peut être saisie pour avis. Elle avait d'ailleurs invité le Parlement à s'interroger, dans le cadre des débats sur le projet de loi relatif à la gestion de la crise sanitaire, sur des garanties supplémentaires à adopter pour respecter les principes d'éthique et de proportionnalité quant à la généralisation du passe sanitaire. [107]

Elle peut également mener des contrôles dont la sanction pécuniaire n'est pas la seule issue. Elle s'efforce dans un premier temps, d'accompagner avec pédagogie les acteurs de la santé, au soutien d'un traitement conforme et éthique des données de santé *(A).* En second lieu, elle dispose d'un rôle sanctionnateur (*B*), comparable à celui d'un tribunal.

A) Un rôle de contrôle, soutenu par des considérations pédagogiques

Le 25 mai 2018 a marqué un tournant dans l'organisation des établissements de santé. Depuis ce moment, les contrôles des agents de la CNIL se font plus nombreux (384 en 2021)[108]. La Commission, après une plainte, un signalement, sur son initiative ou lors du programme annuel de contrôles, peut, sur décision de sa présidente Marie-Laure Denis, effectuer quatre types de contrôle : sur place, sur pièces, en ligne ou sous forme d'audition sur convocation.

Le Covid 19 a mis en exergue des pratiques douteuses de collecte des données de santé, conduisant la CNIL à développer une stratégie de contrôle, « *pour répondre aux défis posés par le contexte sanitaire, notamment en termes de sécurité des données de santé »* selon ses termes.

A ce titre, le 4 octobre 2021, la Commission a mis en demeure la société Francetest pour sécurisation insuffisante des données de santé.

---

[107]Audition devant la Commission des lois du Sénat sur le projet de loi relatif à la gestion de la crise sanitaire. Propos liminaire de Marie-Laure Denis, présidente de la CNIL, mercredi 21 juillet 2021

[108]Présentation du rapport d'activité 2021 et des enjeux 2022 de la CNIL – 42ème Rapport annuel 2021, CNIL, 11 mai 2021

Selon la CNIL, « *Une mise en demeure est une injonction du Président de la CNIL adressée à un responsable de traitement ou à un sous-traitant, de cesser un ou plusieurs manquement(s) constaté(s) au Règlement général sur la protection des données (RGPD) dans un délai fixé. Elle intervient après une plainte reçue par la CNIL ou un contrôle (en ligne ou sur place) effectué auprès d'un organisme.* » Cela ne constitue pas une sanction, et intervient comme avertissement dans la chaine répressive de la CNIL. En l'espèce, Francetest est une société sous-traitant avec 350 officines en France, et permettant la gestion simplifiée des données personnelles des patients ayant effectué un test antigénique. Elle simplifie l'envoi des résultats et leur publication sur SI-DEP, la plateforme du ministère des solidarités et de la santé centralisant les résultats de ces tests. Après un signalement anonyme et des contrôles, la CNIL conclut à la violation de la base de données médico-administratives de Francetest, (dont le numéro de sécurité sociale (NIR))de 386 970 personnes sont concernées) En dépit de la prise de « certaines mesures pour corriger le défaut de sécurité qui était à l'origine de la violation de données lorsque la société en a eu connaissance », la CNIL conclue à *« de multiples insuffisances en termes de sécurité, notamment, l'hébergement de données de santé chez un prestataire ne disposant pas d'un agrément HDS, le recours à des processus d'authentification insuffisamment robustes, l'utilisation d'une fonction de hachage faible et une journalisation lacunaire des activités des serveurs du service Francetest. »* Cela constitue un manquement à l'article 32 du RGPD, qui conduira le sous-traitant des 350 pharmacies à devoir se mettre en conformité.

La pédagogie, voire même la patience dont fait preuve la CNIL est remarquable. Elle laisse deux mois à la société pour prendre les mesures de protection adéquates. La Commission prend le soin de lui rappeler que « *la caractérisation du manquement à la sécurité relevé s'effectue tant au regard (…) des données de santé, qui sont des données dites "sensibles" qui nécessitent une protection particulière en application de l'article 9 du RGPD – que du volume de données objet de la violation ainsi que des risques qu'une telle violation fait peser sur les personnes »*[109]. Si cette mise en demeure ne constitue pas une sanction, la CNIL peut aller plus loin dans son rôle de régulateur des données personnelles (*B*).

[109]Décision MED-2021-093 du 4 octobre 2021

B) Un rôle sanctionnateur en cas de non-conformité au RGPD du traitement de données de santé

Une majeure partie du contentieux relatif aux données personnelles, dont les données de santé, est réglée par la CNIL. Le bilan[110] est sans précédent. : en 2021, la CNIL a reçu 14 143 plaintes et en a clôturé 12 522. Elle a procédé à 384 contrôles et les manquements constatés à l'occasion de certaines des instructions menées, ont conduit à prononcer 135 mises en demeure et 18 sanctions, pour un montant cumulé d'amendes jamais atteint. Cette dernière peut en effet, à l'issue de contrôles ou plaintes, prononcer des amendes allant jusqu'à 20 millions d'euros ou 4% du chiffre d'affaires. Ces sanctions peuvent être rendues publiques, altérant souvent la réputation des établissements publics ou entreprises mis en cause.

Un exemple récent nous est donné par la délibération de la formation restreinte de la CNIL du 15 avril 2022 concernant la société DEDALUS BIOLOGIE. [111] Les faits sont les suivants : la société DEDALUS BIOLOGIE commercialise des solutions logicielles à destination de laboratoires d'analyses médicales, appelées solutions de gestion de laboratoire. Environ trois mille laboratoires de biologie médicale privés et entre trente et cinquante laboratoires d'analyses d'établissements publics de santé sont équipés des solutions éditées par la société DEDALUS BIOLOGIE. Le 23 février 2021, l'on apprenait dans la presse que *" les informations confidentielles de 500 000 patients français ont été dérobées à des laboratoires et diffusées en ligne "*. Avait été publié sur des forums de pirates informatiques, un lien de téléchargement vers un fichier contenant les données médico-administratives (nom, prénom, numéro de sécurité sociale, nom du médecin prescripteur, date de l'examen, informations médicales ((VIH, cancers, maladies génétiques, grossesses, traitements médicamenteux suivis par le patient, ou encore des données génétiques))[112] de 491 840 patients des laboratoires équipés des solutions DEDALUS BIOLOGIE.

Sur le fond, le rapporteur relève que la société DEDALUS BIOLOGIE intervient seulement dans la commercialisation des logiciels à destination des laboratoires. Se posait dès lors la question de sa responsabilité dans la fuite de données, puisqu'elle n'agissait qu'en tant que sous-traitant des laboratoires, au sens de l'article 4 point 8 du RGPD. La CNIL prononce une amende administrative de 1 500 000 €, et *« considère que les défauts de sécurité, qui ont*

[110]Présentation du rapport d'activité 2021 et des enjeux 2022 de la CNIL – 42ème Rapport annuel 2021, CNIL, 11 mai 2021
[111] Délibération de la formation restreinte n° SAN-2022-009 du 15 avril 2022 concernant la société DEDALUS BIOLOGIE
[112] https://www.cnil.fr/fr/fuite-de-donnees-de-sante-sanction-de-15-million-deuros-lencontre-de-la-societe-dedalus-biologie

permis la réalisation de la violation de données (…) résultent d'une négligence des règles élémentaires de sécurité des systèmes d'information qui a conduit à rendre accessibles à des tiers non autorisés les données à caractère personnel traitées par la société.» Un manquement à l'obligation d'assurer la sécurité des données personnelles (article 32 du RGPD) est premièrement relevé. Aussi, c'est une décision extrêmement instructive sur la responsabilité des sous-traitants de données de santé et sur le rôle sanctionnateur de la CNIL. Une compréhension de la sanction se fait au regard du rôle de la société, dans le traitement des données de santé que faisaient les laboratoires. Si elle n'est pas à l'origine de la collecte et l'utilisation des données, son activité de sous-traitant lui permet d'« *agir uniquement au nom et sous la responsabilité des laboratoires pour la maintenance du logiciel et, le cas échéant, la migration vers un autre logiciel par exemple.* » La société est alors sanctionnée pour manquement à l'obligation pour le sous-traitant de respecter les instructions du responsable de traitement (article 29 du RGPD). La société a traité des données au-delà des instructions données par les responsables de traitement. Cette affaire a donné lieu à une saisine du Tribunal judiciaire de Paris par la Présidente de la CNIL, qui adopta le 4 mars 2021[113], une décision demandant aux principaux fournisseurs d'accès Internet de bloquer l'accès au site hébergeant le fichier comprenant les 500 000 données des patients.

Eu égard au contentieux grandissant intéressant le droit des données de santé, la CNIL doit évidemment sanctionner les responsables de traitement récalcitrants. En revanche, cela pourrait être en partie évité, car avant de punir, la CNIL est créatrice de droit souple (§2), avec la vocation d'accompagner les acteurs du monde de la santé dans leur usage du numérique.

§2 : Le droit souple édicté par la CNIL

La prévention plutôt que la sanction est la ligne de conduite de la CNIL. La création de référentiels (*A*), invocables devant le juge administratif (*B*) permet de guider les acteurs dans le traitement de données de santé.

A) L'exemple des référentiels

La sensibilité des données de santé conduit la Commission à édicter des référentiels, pour guider les acteurs et apporter une sécurité juridique supplémentaire. Ces outils précisent également le cadre national et celui issu du RGPD, relatif à la protection des données à

[113]TJ Paris, ord. réf., 4 mars 2021, n° 21-51823

caractère personnel. Les référentiels de la CNIL ne sont ni exhaustifs, ni contraignants et s'appliquent au public auquel ils sont destinés. La publication de ces documents par la CNIL correspond aux nouvelles pratiques imposées par le RGPD et la protection accrue des données à caractère personnel. Dans le monde de la santé, secteur en proie à de constantes innovations technologiques, les référentiels de la CNIL font office de « guide » pour les professionnels de santé et les responsables de traitement. Ils servent aussi l'objectif de lisibilité de la règle de droit.

A titre d'illustration, la LIL et le RGPD imposent des obligations pour les cabinets médicaux et paramédicaux. En 2020, la CNIL publie le référentiel relatif aux traitements de données à caractère personnel destinés à la gestion des cabinets médicaux et paramédicaux[114], pris en application des dispositions de l'article 8-I-2-b de la loi du 6 janvier 1978 modifiée. Se faisant, la Commission accompagne les professionnels de santé libéraux dans la mise en conformité des traitements de données de leurs patients. Le référentiel souligne six traitements de données personnels incombant à ces professionnels dans leur exercice :

- La tenue du dossier médical,
- L'établissement et la télétransmission des documents à destination de l'assurance maladie,
- La tenue du dossier de prise en charge sanitaire (comme le dossier de soins infirmiers),
- La télémédecine,
- La prise de rendez-vous médicaux,
- La tenue de la comptabilité

A chacune de ces finalités, le référentiel indique une base légale que le professionnel de santé pourra envisager pour légitimer son traitement dans le registre des traitements de données personnelles, qu'il est tenu de tenir en vertu de l'article 30 du RGPD.

Plus récemment, la CNIL a publié un référentiel sur les entrepôts de données de santé, suite à l'adoption d'une délibération en date du 7 octobre 2021[115]. Les entrepôts de données de santé sont des bases de données destinées à être utilisées notamment à des fins de recherches, d'études ou d'évaluations dans le domaine de la santé, dont le régime est par principe, soumis à autorisation de la Commission. Afin de simplifier les démarches, la CNIL a adopté ce

[114]Référentiel relatif aux traitements de données personnelles pour les cabinets médicaux et paramédicaux, CNIL, 28 juillet 2020
[115]CNIL, délibération 2021-118 du 7 octobre 2021

référentiel lorsque des organismes souhaitent conserver des données sensibles de santé à l'occasion de l'exercice d'une mission d'intérêt public, au sens de l'article 6.1.e du RGPD. Cela est une condition *sine qua non* pour respecter le périmètre du référentiel. Pris en application du RGPD et des règles du CSP, le référentiel permet à des hôpitaux notamment de conserver en interne, les données de santé de leurs patients à des fins de réutilisation pour la recherche et l'innovation. L'Hôpital Foch à Suresnes (92) ou encore l'Assistance Publique-Hôpitaux de Paris (AP-HP) disposent de leur propre base de données médicales, leur permettant ainsi d'accéder directement aux données concourant à l'amélioration de la prise en charge des patients ou l'accélération de la recherche.
Source de simplification pour les acteurs de la santé, les référentiels se sont vu reconnaitre par le Conseil d'État, le statut de « soft law » *(B)*

B) La reconnaissance de l'invocabilité du droit souple : une nouvelle méthode de régulation des données de santé

Dans un avis du 7 décembre 2017[116], le Conseil d'État observe que *« la CNIL se voit attribuer le pouvoir d'adopter de nouveaux instruments de droit souple : lignes directrices, recommandations, référentiels, codes de conduite, dispositifs de certification… »* Le recours à des instruments dits de droit souple ou « soft law », dont la force normative et les effets juridique sont discutés, est encouragé par le Conseil d'État, notamment dans le cadre de l'adaptation du droit national au cadre juridique européen en matière de protection des données. Ainsi, les référentiels de la CNIL, ainsi que tous les actes de droit souple qu'elle édicte, sont invocables devant le juge administratif dans le cadre d'un recours pour excès de pouvoir, au même titre que les actes de droit mou des autorités de régulation.
C'est ce qu'a jugé le Conseil d'État dans un arrêt 21 mars 2016, Société Fairvesta International GMBH et autres[117], qui renverse la théorie administrativiste selon laquelle il n'est possible de contester un acte administratif devant le juge à la seule condition que celui-ci produise des effets juridiques.

Dès lors, des recours peuvent alors être intentés par des institutions qui se seraient vu refuser la création d'un entrepôt de données de santé, sur le fondement du référentiel du 7 octobre 2021 ci-dessus cité. La contrepartie de l'invocabilité du droit souple de la CNIL devant le

[116] Avis sur un projet de loi d'adaptation au droit de l'Union européenne de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés
[117] N °368082

juge administratif, est l'appréciation qu'il peut porter sur la portée de celui-ci. Ainsi, le Conseil d'État, saisi au contentieux par des tiers, est à même de se prononcer sur l'objet, la portée, la validité des instruments adoptés par la Commission.
Mais, le rôle du Conseil d'État dans le traitement des données de santé se retrouve surtout au stade du contrôle qu'il opère.

L'étude de l'office du juge dans le traitement des données de santé nous conduit donc à envisager une seconde section sur la place des juridictions dans le contrôle du traitement des données de santé (Section II).

Section II : La place des juridictions dans le contrôle du traitement des données de santé

Le considérant 4 du RGPD dispose que : *« Le droit à la protection des données à caractère personnel n'est pas un droit absolu ; il doit être considéré par rapport à sa fonction dans la société et être mis en balance avec d'autres droits fondamentaux, conformément au principe de proportionnalité. »*[118] Et précisément, le RGPD autorise le traitement de données de santé, si le consentement explicite des personnes est donné lorsque les circonstances le justifient. Les juridictions se portent alors garantes de l'effectivité des recours visant à protéger les données de santé (§1) si tant t'est qu'elles soient compromises. Enfin, pour consolider la protection des données de santé, une lisibilité accrue de leur cadre juridique est à préconiser (§2).

§1 : Les juridictions garantes de l'effectivité des recours visant à protéger les données de santé

A) Les apports du juge de cassation dans la protection des données de santé

La protection des données de santé est un sujet dont Jean- Marc Sauvé, vice-président du Conseil d'État s'est saisi en 2017 : *« Dans ce contexte singulier – sensibilité particulière de ces données et intérêt de leur exploitation et de leur partage –, les données de santé font l'objet d'une protection qui tient compte de leur spécificité mais dont l'équilibre a été récemment revu pour assurer une conciliation plus adaptée entre le nécessaire respect de la vie privée des personnes physiques et la poursuite d'objectifs légitimes de santé publique. »* Il est reconnu par la Haute juridiction administrative l'intérêt et la nécessité de protéger les données de santé, en raison de leur sensibilité ; qui a même tenté de les définir en 2010, en

[118]Considérant 4 du RGPD

considérant que constitue une donnée de santé, une donnée donnant une « *information sur la nature, la durée, ou la gravité* » d'une affection. [119] Les interventions du juge de cassation dans la protection des données de santé se font de plus en plus nombreuses, corrélativement au degré d'atteinte qui y est porté.

A ce titre, la crise sanitaire a nourri le contentieux du droit des données de santé. Les municipalités et services publics ont fait usage durant le Covid 19, de caméras thermiques, permettant de mesurer la température corporelle des personnes. La CNIL s'est opposée à cette pratique, considérant que la fièvre n'est pas un symptôme systématique de la maladie, que la détection du virus par le biais de ces caméras intelligentes est vaine, puisque certains malades sont asymptomatiques[120]. Au Conseil d'État, saisi en référé par la Ligue des Droits de l'Homme[121] de confirmer la position de la Commission. La commune de Lisses a porté atteinte au droit au respect de la vie privée des élèves et du personnel des écoles de la ville, soumis systématiquement à un test de fièvre à l'entrée. De plus, les caméras collectent des données de santé, sans leur consentement, contrairement à ce qu'exige la LIL et RGPD. Cette collecte non conforme, constitue un traitement automatisé de données personnelles. En l'absence de raison de santé publique, et surtout en l'absence de consentement des élèves et du personnel de l'école, la Commune porte, selon le juge des référés, une atteinte grave et manifestement illégale[122] au droit au respect de la vie privée comprenant le droit à la protection des données personnelles et la liberté d'aller et venir. En plus de l'appréciation portée sur la légalité de l'installation de caméras thermiques par les municipalités en temps de crise sanitaire, le Conseil d'État apporte une nouvelle définition du traitement des données de santé : « *Ce traitement, s'il porte sur des personnes identifiables et dès lors qu'il vise à apprécier l'état d'un paramètre significatif de leur état de santé au regard d'une pathologie particulière, porte sur des données personnelles de santé. »* Une définition qui permettra une meilleure compréhension pour les acteurs de la santé.

Il paraissait important, en sus du contrôle opéré par le Conseil d'État, de souligner l'apport de la Cour de cassation dans le droit des données de santé. Un exemple récent nous donne sa position sur l'accès à ses données médicales d'un patient.[123] La Cour rappelle qu'il existe une

[119]Conseil d'État, 10ème et 9ème sous-sections réunies, 19/07/2010, n° 334014.
[120]Caméras dites « intelligentes » et caméras thermiques : les points de vigilance de la CNIL et les règles à respecter, 17 juin 2020
[121]Conseil d'État, Ordonnance du 26 juin 2020, Caméras thermiques à Lisses, n° 441065
[122]Article L 521-2 du code de justice administrative
[123] Cour de cassation, civile, Chambre civile 2, 30 septembre 2021, n°19-25.045, Publié au bulletin

différence entre le droit d'accès à son dossier médical au sens du CSP[124] et le droit d'accès au sens du RGPD. Ainsi, le patient qui souhaitera obtenir ses informations médicales, aura plus d'intérêt à mobiliser l'article L1111-7 du Code de la santé publique, qui dispose que « *Toute personne a accès à l'ensemble des informations concernant sa santé détenues, à quelque titre que ce soit, par des professionnels et établissements de santé »,* plutôt que l'article 15 du RGPD. Le délai est plus court via le CSP (huit jours, contre un mois en sollicitant l'article 15 du RGPD), et le patient n'aura pas à payer les frais d'accès mentionnés par le RGPD, et ne se verra pas restreindre son droit, en vertu de l'article 15.4 du RGPD qui permet de le faire afin de ne pas porter atteinte « *aux droits et libertés* »[125] d'autrui.

L'intérêt porté par le juge européen au droit des données de santé n'est guère étonnant, dans la mesure où le RGPD est un instrument juridique européen. La recherche d'un équilibre entre l'ouverture de l'accès aux données et la protection de la vie privée des personnes relève alors de son contrôle. *(B)*

B) La recherche d'un équilibre entre l'ouverture de l'accès aux données de santé et la protection de la vie privée des personnes par le juge européen

Sur le plan politico-juridique d'abord, la recommandation n° R (97) 5 relative à la protection des données médicales du Comité des ministres du Conseil de l'Europe[126] énonce un lien étroit entre protection des données de santé, respect de la vie privée et secret professionnel. Ainsi, en son point 3.2, elle préconise que le traitement des données de santé ne soit autorisé qu'aux seuls *« professionnels des soins de santé ou les personnes ou organismes agissant pour le compte de professionnels des soins de santé – soumises aux « règles de confidentialité propres aux professionnels de santé »* c'est-à-dire au secret médical. Très classiquement, il est opéré dans la recommandation, une proportionnalité entre les risques du traitement des données de santé eu égard au respect de la vie privée, le tout couvert par le secret médical.

La CEDH, par la balance qu'elle opère entre les intérêts de protection des données de santé et le but légitime poursuivi par leur divulgation, contribue à développer la définition de la donnée de santé. Ainsi, sont de telles données, les « *informations relatives à la séropositivité*

[124]Article L 1111-7 du Code de la santé publique
[125] Article 15.4 RGPD
[126] Recommandation R (97) 5 du Comité des ministres aux états membres relatives à la protection des données médicales (adoptée par le Comité des ministres le 13 février 1997, lors de la 584e réunion des délégués des ministres)

d'une personne »[127], les « *informations sur la santé mentale d'un individu* »[128] ou celles « *relatives à un avortement* ».[129] Au visa de l'article 8 de la Convention, l'étendue de la protection opérée par le juge européen est remarquable. Elle concerne par exemple, la protection de la vie sexuelle comme dans l'arrêt Z c/ Finlande de 1997, où le juge conclue que la divulgation de la séropositivité d'une femme à l'occasion d'un procès intenté à son époux, viole l'article 8. Mais, elle concerne également la protection de la vie intime des femmes, comme dans l'arrêt Konovalova c. Russie (2014) à l'issu duquel un hôpital public russe est condamné pour avoir divulgué des informations de santé d'une mineure souhaitant avorter après un viol.

La CEDH impose aux États de ménager une législation interne permettant de garantir aux individus la protection de leurs données à caractère personnel lorsque ces dernières doivent être divulguées. Ainsi, la balance entre vie privée et but légitime de la divulgation ne serait qu'à l'équilibre si l'ingérence ne soutenait qu'un intérêt public hautement important. A ce titre, lorsqu'au cours de procès, une donnée médicale non autorisée est divulguée par la partie adverse, le juge européen, en dépit de l'intérêt de la Justice, ne tolérera pas une telle immixtion.[130]

Ainsi, la Cour se tare de pouvoir *« non seulement (…) protéger la vie privée des malades, mais également (…) préserver leur confiance dans le corps médical et les services de santé en général* » au moyen d'une sollicitation quasi-constante de l'article 8 de la ConvEDH dans les affaires intéressant les données de santé.

La protection des données de santé, qu'elle passe par la CNIL ou les juges, ne serait que pleinement effective qu'au regard d'une lisibilité complète de son encadrement juridique (§2).

§2 : La lisibilité de l'encadrement juridique du droit des données de santé : initiatives françaises et européennes

La simplification du droit des données de santé par le RGPD est en marche. Mais, elle s'oppose encore, pour les acteurs de terrain, avec le manque de lisibilité de la règle de droit : confusion base légale et exception, difficulté de recueil du consentement au traitement des données, positionnement délicat dans le partage et l'échange des données…

---

[127]Biriuk c. Lituanie, 2008, § 39
[128]Mockutė c. Lituanie, 2018, § 94
[129]M.S. c. Suède, 1997, §§ 41-42
[130]; L.L. c. France, 2006 (§§ 32-48)

Il devient opportun de clarifier les choses du point de vue déontologique *(A)* et de se projeter vers une « *harmonisation des utilisations des données de santé »* [131] (*B*).

A) Les difficultés constatées par les professionnels de santé dans la compréhension du régime du traitement des données de santé : vers une création d'une section éthique des données au sein du Code de déontologie médicale ?

Il ressort principalement des recherches menées dans le cadre de ce mémoire, la nécessité d'offrir un cadre déontologique à la e-santé, en créant une section dédiée à l'éthique du numérique en santé dans le Code de déontologie médicale. Cela est en réflexion au sein du Conseil National de l'Ordre des médecins qui, sur les recommandations de l'État, a dans un premier temps songé à la création d'un code d'E-déontologie. Cette proposition a été appuyée par la Cellule Ethique du Numérique en Santé du Ministère de la santé, qui préconise de « *de relire le code de déontologie médicale afin de vérifier l'impact du numérique en santé sur les articles et les commentaires du code* ».[132] Le Code de déontologie médicale, en vigueur depuis 1995[133], « *est le reflet de la vision morale, éthique et juridique d'une époque révolue et ne tient pas compte des évolutions technologiques récentes* » selon le Docteur Loïc Etienne, médecin urgentiste et précurseur des questions de la e-santé.

Finalement, au code d'E-déontologie, a été préférée la création d'un nouvel article 13-1 dédié à l'e-santé dans le Code de déontologie médicale. Selon le Docteur Anne-Marie Trarieux, présidente de la section éthique et déontologie du Cnom, *« le code de déontologie médicale doit intégrer les changements qu'apportent les nouvelles technologies. L'e-santé est source de nombreux espoirs. Elle facilite la coordination des soins autour du patient (…) Mais elle est aussi source d'inquiétudes, elle (…) transforme les parcours de soins et bouscule ce qui fait la relation médecin-patient, le secret médical, le respect de la dignité humaine, l'indépendance des professionnels de santé…* »[134] Ce qui justifie que le Cnom ne veuille pas, pour l'heure, introduire de nouvelles règles déontologiques spécifiquement relatives aux données de santé, mais préfère adapter l'existant. Ainsi, « *actuellement l'Ordre travaille à la révision des commentaires de l'article 4, relatif au secret médical, où figure un paragraphe consacré aux évolutions technologiques et numériques.* ». Il semble donc que l'ajout d'une

[131]Douville T. ; La construction d'un espace européen des données de santé Thibault Douville, Recueil Dalloz 2022 p.1304
[132] Doctrine technique du numérique en santé, 2019

[133] Décret n° 95-1000 du 6 septembre 1995 portant code de déontologie médicale
[134]Donner un cadre déontologique à l'e-santé, M LE BULLETIN ÉDECINS

section complète sur la e-santé ne soit pas actuelle et que les difficultés rencontrées par les professionnels de santé face à la digitalisation de la santé soit réglée grâce à la formation et aux outils du Cnom. En effet, ce dernier accompagne les médecins depuis 2018 grâce à des guides et des fiches sur la protection des données, et ce afin de renforcer les obligations et devoirs des professionnels face aux données de santé.

Pour l'heure, et même si la crise sanitaire a démontré le bien-fondé des outils technologiques dans le monde de la santé, l'introduction du numérique en santé dans le Code de déontologie gagnerait à être accélérée. Au niveau européen en revanche, le droit des données de santé connait un renouveau avec la récente proposition d'un espace européen des données de santé (*B*).

B) La proposition de règlement relatif à la construction d'un espace européen des données de santé

L'adaptation du droit français au nouveau cadre européen s'est faite en plusieurs étapes par les modifications apportée à la LIL, par la loi du 20 juin 2018, puis par son décret d'application, par décret du 1er août 2018, puis par la réécriture et la mise en cohérence de cette loi, par l'ordonnance du 12 décembre 2018 ; et enfin par l'élaboration d'un nouveau décret d'application de la loi, daté du 29 mai 2019 et entré en vigueur le 1er juin. Si la loi de 1978 a subi modifications et révisions, le RGPD lui n'a fait l'objet d'aucune réforme depuis 2016, en dépit de propositions de la doctrine. Au-delà d'une refonte du RGPD, il apparaît urgent de préciser et rendre lisible le cadre juridique du traitement des données de santé par un encadrement novateur, au plan européen.

C'est ainsi que le 3 mai 2022, la Commission Européenne annonce le lancement d'un Espace européen des données de santé (EHDS)[135], vu selon elle comme « *une pierre angulaire dans la construction d'une union européenne de la santé forte* »[136] L'objectif est triple : construire un « marché unique des produits et services de santé numérique », apporter « un cadre cohérent, fiable et efficace pour l'utilisation des données de santé à des fins de recherche, d'innovation, d'élaboration des politiques et de réglementation » tout en garantissant la protection des données personnelles des personnes grâce aux normes élevées de l'Union en la matière.

[135] Proposition de règlement du Parlement européen et du Conseil, relatif à l'espace européen des données de santé, COM(2022) 197 final, 03/05/2022

[136]Commission européenne - Communiqué de presse, Union européenne de la santé: Un espace européen des données de santé pour les personnes et pour la science Bruxelles, le 3 mai 2022

La proposition de règlement portée par la Commission s'appuie sur les articles 16 et 114 du TFUE, sur le RGPD, sur le Règlement sur les données du 23 février 2022[137] et sur l'Acte sur la gouvernance des données, approuvé par le Conseil le 16 mai 2022[138]. Ce texte vise « *à promouvoir la disponibilité des données et à créer un environnement fiable pour faciliter leur utilisation à des fins de recherche et de création de nouveaux services et produits innovants.* »[139] Pas étonnant donc, qu'il soit le pilier du futur EHDS. En effet, ce dernier permettra pour tous les citoyens européens, un accès et un partage simplifié de leurs données de santé, avec les professionnels de santé des États membres. Les dossiers patients, ainsi que leurs prescriptions, leurs examens médicaux, leurs résultats de laboratoire etc… seront édités dans un format commun européen. Des autorités de santé numérique seront désignées par chaque État membre, qui participera à une infrastructure numérique transfrontière : MyHealth@EU. Objectif assumé : aider les patients à partager leurs données de santé hors les frontières de leur État. L'européanisation des données de santé est en route, et cela ne sera pas sans servir les intérêts de la recherche médicale puisque qu'un cadre juridique commun sera créé pour l'utilisation des données de santé à des fins de recherche, d'innovation, de santé publique, d'élaboration de politiques et de réglementation. Un mécanisme d'autorisation pour l'accès aux données de santé sera mis en place, chapeauté par un organisme responsable de cela dans chaque état membre. La Commission Européenne souligne que « *l'accès ne sera autorisé que si les données demandées sont utilisées à des fins particulières, dans des environnements fermés et sécurisés et sans que l'identité des personnes ne soit révélée* »[140]. De quoi rassurer les Européens… dont les données de santé risquent de transiter par le HealthData@EU, nouvelle infrastructure décentralisée de l'UE, qui servira à la réutilisation secondaire des données de santé dans le cadre de projets transfrontaliers.

Si le cadre juridique qui viendra préciser ces échanges et partages européennes de données n'est pas précisé, l'on ne peut qu'espérer qu'il offrira des garanties élevées de protection de la vie privée ainsi que peut être qu'il créera de nouveaux droits en faveur des personnes.

---

[137]Règlement du Parlement européen et du Conseil fixant des règles harmonisées pour l'équité de l'accès aux données et de l'utilisation des données COM(2022) 68 final

[138]Règlement du Parlement européen et du Conseil portant sur la gouvernance européenne des données et modifiant le règlement (UE) 2018/1724

[139]Conseil de l'UE - Communiqué de presse, Le Conseil approuve l'acte sur la gouvernance des données, 16 mai 2022

[139]Commission européenne - Communiqué de presse, Union européenne de la santé: Un espace européen des données de santé pour les personnes et pour la science Bruxelles, le 3 mai 2022

En France, le Conseil d'Etat se prononcera certainement sur le futur Espace européen des données de santé. Si l'intérêt général et la protection des droits et libertés fondamentaux seront objet de son avis et/ou contrôle, il s'agira également de se prononcer sur l'échange et le partage des données outre nos frontières. Cela ne devrait pas poser de problème à la juridiction administrative qui a jugé dans une ordonnance en référé du 13 octobre 2020[141] que *« confier le traitement des données de santé à la société Microsoft dans le cadre de la Plateforme des données de santé ne constitue pas une atteinte grave et manifestement illégale au droit au respect de la vie privée et au droit à la protection des données personnelles au sens de l'article L 521-2 du Code de justice administrative »* ne justifiant ainsi pas, la suspension du Health Data Hub, controversé pour les relations qu'il entretenait avec la société américaine Microsoft.

[141]Conseil d'État, Juge des référés, 13/10/2020, 444937, Inédit au recueil Lebon

Conclusion

La sensibilité des données de santé justifie un principe général d'interdiction de leur traitement informatique. Pourtant, et partout, il est constaté une collecte généralisée de données de santé, en parallèle de l'accélération du numérique en santé.

Le premier constat est donc la malléabilité des articles 9 du RGPD et 6 de la LIL qui organisent le régime juridique d'interdiction du traitement des données de santé. Affaiblie par les exceptions qui la complète, cette interdiction est levée au profit des enjeux de santé publique et de recherche médicale. Pour autant, la LIL et le RGPD offrent un cadre protecteur aux données de santé, permettant une utilisation de ces dernières, justifiée par la prise en charge du patient à l'hôpital, les besoins de la recherche, les impératifs de santé publique et la gestion des données par les organismes publics dont les autorités sanitaires. Cela n'est pas à remettre en cause, et est même à plébisciter, car sans partage de données de santé, il n'y a point de soins.

En revanche, il est utile de se demander si le consentement de la personne au traitement de ses données de santé existe encore et si celui-ci, mis à part des cas dérogatoires, n'est plus qu'un mythe juridique. Nous avons souligné qu'il pouvait être contourné à de nombreux égards, et que la personnalité du droit de consentir peut-être mise à mal par les nombreuses exceptions au principe d'interdiction du traitement des données de santé. Hors les cas de recherche ou de partage de données hors équipe de soins, que reste-t-il du consentement du patient au traitement de ses données de santé ? Le droit français considère aujourd'hui la donnée de santé, comme un « accessoire » du corps humain. Elle tombe sous le coup du principe d'indisponibilité du corps humain, consacré par l'article 16-1 du Code civil, et l'idée d'une patrimonialité des données n'en est qu'au stade de l'émergence aux vues des obstacles éthiques et juridiques que cela représenterait. Le droit sur ses propres données de santé n'est donc pas consacré, et il est évident que ces dernières peuvent vite nous échapper. Plus que jamais après la crise sanitaire, le secteur de la santé est une cible particulièrement vulnérable, du fait notamment de la recrudescence des attaques informatiques à l'égard des établissements de soins. Alors, à défaut d'un droit offrant tout contrôle aux personnes sur leurs données, il faut croire en l'éthique et la responsabilisation des acteurs du traitement des données de santé, ainsi qu'en l'arsenal répressif déjà existant pour les protéger.

Le second constat est que la règle de droit est complexe à appréhender par les professionnels de santé, par les établissements, et par les personnes concernées par le traitement de leurs données de santé. Le 23 février 2022, la Commission Européenne présentait le Data Act également nommé Loi sur les données, visant à combler les lacunes de l'actuel RGPD et permettant, entre autres, de réguler les données industrielles. Aussi, le Data Governance Act approuvé à la fin de l'année 2021, permettra de réutiliser les données de santé du secteur public à plus grande échelle. Le vote de ces textes répond également au besoin d'uniformisation du droit des données personnelles, dont le corpus juridique s'étoffe constamment. La priorité demeure donc de continuer à sensibiliser, former et responsabiliser les responsables de traitement à l'usage qu'ils font des données. A ce titre, les DPD et les DSI des établissements de santé occupent une place déterminante parmi les métiers de l'hôpital de demain.

Conclure sur un tel sujet parait être difficile tant les défis du traitement des données de santé sont grands et cristallisent l'ensemble des inquiétudes du juriste. Pour preuve, depuis juillet 2021, un Service Européen de Santé en Ligne (Sésali) permet aux professionnels de santé français d'accéder aux synthèses médicales de patients provenant de sept pays membres de l'UE (Espagne, Luxembourg, Estonie, Croatie, Malte, République Tchèque et Portugal). L'intimité de l'information sur la santé n'a plus de frontière. Paradoxalement, cela n'inquiète pas les citoyens car il demeure important de pouvoir se faire soigner hors de son lieu de vie habituel. Comme évoqué, la protection des données de santé n'est plus seulement une affaire nationale. C'est donc aux acteurs européens de continuer à œuvrer à l'équilibre de la balance recherchée entre protection de la vie privée et partage et échange des données de santé.

Entre enjeux d'accès aux données de santé et régulation des acteurs ayant le besoin d'en connaitre, entre partage des données au bénéfice des progrès médicaux et protection des données de santé, les institutions politiques et juridiques jouent un rôle central. Il s'agit pour elles de centraliser les besoins et objectifs du numérique en santé, mais également de trouver le juste équilibre entre exploitation et sécurité des données de santé.

Parfois préoccupant, l'essor du traitement des données de santé présente des bénéfices indéniables pour l'amélioration des soins et le développement de nouvelles pratiques médicales. Il ne reste plus qu'à espérer que cet essor sera l'occasion pour les pouvoirs publics d'engager une discussion autour du consentement au traitement des données de santé, dont les contours juridiques demeurent flous.

Annexes

Annexe 1 : Questionnaire sur le consentement des patients au traitement de leurs données de santé : réponses des usagers de la Polyclinique Saint Laurent (35)

Questionnaire aux patients de la Polyclinique St Laurent
Le consentement au traitement de vos données de santé

Préambule : Les personnes dont les données de santé sont collectées disposent de droits, dont celui d'être informées. Il peut s'agir de vous, patients, ou de personnes participant à une recherche. L'information vous permet de conserver la maîtrise des données vous concernant. C'est une obligation prévue par le Règlement général sur la protection des données (RGPD) qui protège les données personnelles en Europe.

Les données de santé sont les données personnelles **relatives à la santé physique ou mentale d'une personne physique qui révèlent des informations sur l'état de santé de cette personne**.

Ainsi, les données de santé regroupent des informations :

Collectées lors de la prestation d'un service de soins de santé

Recueillies lors d'un examen de santé

Concernant une maladie ou un handicap

Avez-vous lu la partie « Règlement général de protection des données » du livret d'accueil de la Polyclinique ? Si oui, trouvez-vous cela compréhensible ?

5 patients ont répondu « non » à cette question, en soulevant pour la plupart que le livret d'accueil n'était pas présent dans leurs chambres.

Un patient a répondu qu'il l'avait lu lors d'un précédent séjour.
Un autre a répondu « oui » mais préconise d'expliciter la notion de « RGPD ». Ce même patient propose d'afficher dans les chambres, la partie RGPD du livret d'accueil.

Connaissez-vous vos droits en matière de données à caractère personnel ?

3 « oui » / 4 « non »

Sans de plus amples informations, les patients n'ont pas du tout développé. Cette question était certainement trop fermée.
Un patient a tout de même listé quelques droits qu'il connaissait comme le droit d'information, de rectification, d'accès à ses données.
Un autre patient déplore que la clinique n'organise pas de réunions ou de sessions d'information sur les données à caractère personnel.

Pensez-vous que les données médicales sur votre état de santé, votre prise en charge, vos traitements sont conservées (Vos informations personnelles) ? Si oui, dans quel but ?

Différentes réponses ont été apportées ici : Les patients associés à ce questionnaire savaient, pour la plupart, que leurs données étaient conservées. Ils ont avancé des buts différents pour justifier cela :
Pour faire avancer la recherche médicale
Pour que la polyclinique ait toutes les données lors d'une prochaine hospitalisation
Pour des raisons médicales
Pour le suivi de leur état de santé

A juste titre, un patient a soulevé que le droit d'accès à ses données médicales était une obligation réglementaire pour la polyclinique. Ce dernier semblait s'intéresser de près au sujet.

Un autre patient est favorable à la conservation de ses données : souffrant d'une lourde pathologie, cela évite selon lui, une redondance d'examens médicaux et permet de suivre l'évolution de sa maladie.

Savez-vous qui et comment peut avoir accès à vos informations de santé lors de votre séjour ? Et même après votre sortie ?

A cette question, quelques patients semblaient avoir conscience que des professionnels pouvaient accéder à leurs informations de santé lors de leur séjour et après leur sortie. Ils ont cité :
Leur médecin de famille
Les spécialistes et les pharmaciens
L'ARS, les autorités de santé, les organismes publics
Les médecins en général
Les psychiatres/psychologues
Les cadres de santé
Le personnel de soin de Saint Laurent

D'autres ne savaient pas du tout que l'accès à leurs informations de santé était possible après leur sortie.
Un patient souligne ici qu'il peut lui-même accéder à son dossier, sur demande.

Que pensez-vous du Dossier médical partagé ? (Le ***Dossier*** Médical ***Partagé*** (DMP) est un carnet de santé numérique qui conserve et sécurise vos informations de santé : traitements, résultats d'examens, allergies... Il vous permet de les ***partager*** avec les professionnels de santé de votre choix, qui en ont besoin pour vous soigner)) Etes-vous favorable à ce type d'outil ? Si oui/non, pourquoi ? **A titre d'information, le DMP deviendra systématique à compter de 2022.**

Cinq patients n'ont pas répondu à la question : « Que pensez-vous du Dossier médical partagé ? » Deux s'y montrent favorables.

En revanche, certains ont émis leur avis personnel. Pour ceux qui voient un intérêt au DMP, les raisons avancées sont les suivantes :
« Utile en cas d'urgence »
« Favorable à cet outil à condition qu'il soit protégé par le secret médical »
« Utile car pas besoin de redire ses informations s'il arrive quelque chose »

Quatre patients soulèvent la volonté d'avoir accès à leur DMP, à n'importe quel moment.
Un patient souligne l'importance de ne pas divulguer ce DMP aux assurances, banques, et toute entreprise hors médical. Ce même patient est rassuré par un tel outil. Il pense en effet, que lors de malaises, le SAMU aura directement accès à sa pathologie et son traitement.

Voyez-vous un risque au partage de vos informations de santé, dans le cadre de votre prise en charge ? Ou au contraire, voyez-vous un bénéfice à l'échange et au partage de vos données ?

Les sept patients interrogés soulignent le bénéfice que procure pour les professionnels de santé, le partage des informations de santé. Soucieux de leur protection, ils insistent sur le fait que cela doit demeurer dans le contexte médical.

Un patient soulève la volonté d'avoir une liste exhaustive des professionnels avec qui sont partagées ses informations.

Merci de votre participation,
Le service Délégué à la Protection des données (DPD),
Mathilde Grente, stagiaire M2 Droit de la santé – Délégué à la protection des données
Les représentants des usagers

Annexe 2 : Synthèse et recommandations formulées à la polyclinique Saint Laurent suite aux réponses des patients au questionnaire

Synthèse et recommandations – Etude sur les données personnelles des patients

L'étude réalisée sur le consentement des patients au traitement de leurs données de santé a permis de mettre en lumière l'interprétation qu'ils ont de leurs droits.

A ce titre, les recommandations suivantes pourraient être étudiées, voire même mises en œuvre.

1. **Côté Qualité : Le livret d'accueil**

Au sein de l'établissement, une procédure dédiée à la diffusion du livret d'accueil est mise en place. Cependant, l'étude démontre qu'un certain nombre de livrets d'accueil n'est pas remis à l'arrivée des usagers.

Propositions d'actions :

- Réviser la procédure « diffusion du livret d'accueil. »
- Revoir avec le RAQ comment la diffusion de la procédure est réalisée
- Contrôler l'application de la procédure

2. **Côté Usagers : Communication**

Propositions d'actions :

- Afficher des informations RGPD et données personnelles dans chaque aile de bâtiment de chaque étage, au même titre que les informations sur la personne de confiance, les directives anticipées…
- Mettre en place des groupes de paroles « Protection des données personnelles », au travers des référents RGPD. → *Exemple de GP : « La protection de vos données à la Polyclinique St Laurent », « Comment faire valoir ses droits garantis par le RGPD au sein de la Polyclinique St Laurent »…*
- Inclure dans la notice d'information RGPD des patients, un exemple d'un acteur pouvant avoir accès à leurs données

3. **Côté professionnels de santé : Information et sensibilisation à la protection des données personnelles**

Propositions d'actions :

- Mettre à disposition un mémento RGPD, sur le modèle de celui proposé par le Ministère de la santé et la DGOS (*« Mémento RGPD à l'usage du directeur d'établissement).* Ce dernier pourrait être proposé par le DPO.
- Mener des campagnes de sensibilisation au RGPD au sein de Saint-Laurent

Annexe 3 : La partie RGPD du livret d'accueil de la polyclinique Saint Laurent

LIVRET D'ACCUEIL

POLYCLINIQUE SAINT-LAURENT

RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES (RGPD)

OBJET DU TRAITEMENT

Les informations recueillies lors de votre consultation ou de votre hospitalisation dans notre établissement font l'objet de traitements informatiques destinés à faciliter votre prise en charge au sein de celui-ci. Le ou les traitements informatiques sont destinés à des fins de médecine préventive, de diagnostics médicaux, de la prise en charge sanitaire ou sociale ou de la gestion des systèmes et des services de soins de santé (cf. article 9.2.h du Règlement général sur la protection des données).

Par ailleurs, certaines informations doivent être transmises aux différents organismes de l'Etat ou d'assurance maladie à des fins de contrôle de l'activité de la Polyclinique Saint-Laurent et de facturation. Le ou les traitements sont destinés à des motifs d'intérêt public dans le domaine de la santé publique ou aux fins de garantir des normes élevées de qualité et de sécurité des soins de santé et des médicaments ou des dispositifs médicaux (cf. article 9.2.i du Règlement européen sur la protection des données ou RGPD) ou le respect d'une obligation légale (cf. article 6.1.c du RGPD).

CATÉGORIES DE DONNÉES

- Identification : noms et prénoms de naissance et usuels, date de naissance, sexe, adresse, numéros de téléphone, courriel*
- Numéro de sécurité sociale (NIR)
- Vie personnelle : habitudes de vie, situation familiale, personnes à contacter*
- Vie professionnelle : employeur*
- Informations d'ordre économique et financier : mutuelle, type de prise en charge
- Données sensibles : santé, génétiques*, ethniques*, religion*, vie sexuelle*

*Données dont la collecte est facultative mais qui permettent d'améliorer la qualité de la prise en charge ou des échanges entre vous et la Polyclinique Saint-Laurent.

SOURCES DES DONNÉES

Certaines de ces données peuvent provenir d'échanges d'informations entre professionnels de santé ou d'échanges d'informations au sein de réseaux sécurisés de soins.

DESTINATAIRES DES DONNÉES

Les données sont réservées aux professionnels de la Polyclinique Saint-Laurent soumis au secret professionnel qui interviennent dans votre prise en charge et peuvent également être mises à disposition de professionnels membres de réseaux de soins. Dans ce cadre, les informations vous concernant sont susceptibles d'être envoyées chez un hébergeur de données agréé ou certifié à cet effet et traitées par des organismes de soins partenaires.

Vos données peuvent être transmises aux organismes publics, autorités de santé, professions réglementées (Trésor public, Agences régionales de Santé, organismes d'assurance maladie et complémentaire, avocats, commissaires aux comptes…) sur demande et dans la limite de ce qui est permis par la réglementation.

Dans le cadre de projets de recherche, la Polyclinique Saint-Laurent est également amenée, après vous en avoir informé individuellement et sauf opposition de votre part, à transmettre des données, préalablement rendues non-nominatives, à d'autres professionnels de santé.

Après vous en avoir informé individuellement et sauf opposition de votre part, vos données peuvent être transmises à des prestataires de services et sous-traitants réalisant des prestations pour la Polyclinique Saint-Laurent (Liste des partenaires en annexe ci-contre).

DURÉE DE CONSERVATION DES DONNÉES

Le dossier médical est conservé, conformément au Code de la Santé Publique, pendant une période de vingt ans à compter de la date du dernier passage, ou au moins jusqu'au vingt-huitième anniversaire du patient, ou pendant dix ans à compter de la date du décès. Certaines données peuvent être conservées plus longtemps si la loi le prévoit.

DROIT DES PERSONNES

Vous pouvez à tout moment accéder aux données vous concernant, retirer votre consentement ou demander l'effacement de vos données en accord avec la réglementation en vigueur. Vous disposez également d'un droit d'opposition sous réserve de motif légitime, d'un droit de rectification et d'un droit à la limitation du traitement de vos données. Par ailleurs, vous pouvez déposer des directives relatives à la conservation, à l'effacement et à la communication de vos données en cas de décès (cf. **www.cnil.fr** pour plus d'informations sur vos droits).

Pour exercer ces droits ou pour toute question sur le traitement de vos données, en première intention nous vous recommandons de contacter notre délégué à la protection des données en joignant une copie de votre pièce d'identité :

Par voie électronique : **cnil@hstv.fr**

Par courrier postal :
Hospitalité Saint Thomas de Villeneuve
Délégué à la Protection des Données
29 Rue Charles Cartel - 22400 Lamballe

En seconde intention vous pouvez vous adresser à la CNIL (cf. **www.cnil.fr**).

Annexe : Liste des partenaires[1]

Pôle Saint-Hélier, Clinique Saint-Yves, Clinique la Sagesse, Hôpital privé de Sévigné, CHP Saint-Grégoire, Pôle Gériatrique Rennais, CHU de Rennes, Hôpital de Montfort-sur-Meu, Hôpital de Bain de Bretagne, Hôpital de Redon, Cabinets de libéraux (Médecins, Infirmiers, Kinésithérapies), Pharmacies, Laboratoires (Novartis, Bayer, Biorance…), Centre d'imagerie Médicale LAËNNEC, Centre Eugène Marquis, Ouest Pathologie, Inzee.care, Doctolib, HAD (Hôpital à Domicile), EHPAD (établissements d'hébergement pour personnes âgées dépendantes), Maisons Médicales.

[1] Dans la réglementation RGPD le terme partenaire correspond au terme sous-traitant.

Liste non exhaustive et susceptible de modification.

Bibliographie

1. *Ouvrages :*

Petit Larousse Illustré 2022, Larousse, 19 mai 2021

BROSSET E, GAMBARDELLA S, NICOLAS G,. La santé connectée et "son" droit : approches de droit européen et de droit français, PUAM, 2017, 241 pages

CALLU M-F, GIRER M, ROUSSET G., Dictionnaire du droit de la santé, Lexis Nexis, 2nd édition, 2021, 462 pages

CORNU G., Vocabulaire juridique, Paris, association Henri Capitant, PUF-Quadrige, 2016

HERVE C., Systèmes de santé et circulation de l'information, Encadrement éthique et juridique, Dalloz, 2006, 208 pages

MOQUET-ANGER M-L., Droit Hospitalier, LGDJ, 6ème édition, 2021, 602 pages

TRUCHET D., Droit de la santé publique, 9 édition, Dalloz, Mémentos, 2016, 340 pages

2. *Mémoires et thèses :*

FALLIGANT L., Le consentement aux soins des personnes vulnérables, Master 2 Droit de santé, Université de Rennes & EHESP, MDSE, 100 pages, 2018

BRASSLET R., La circulation de la donnée à caractère personnel relative à la santé : disponibilité de l'information et protection des droits de la personne. Droit. Université de Lorraine, 517 pages, 2018

VOILLEMET A., L'usage de la donnée médicale, contribution au droit des données, Thèse de doctorat, Université Polytechnique Hauts de France et l'INSA Hauts-de-France, 658 pages, 2022

3. *Articles :*

BERNELIN M., « Les données personnelles de santé des défunts : quelle protection ? » RGDM, n°72, 2019, page 229

BOURDAIRE-MIGNOT C., "2018, l'année du DMP pour tous ? " RGDM, n°66, 2018, page 19

BOURCHIER D., DE FILIPPI P., " Vers un droit collectif sur les données de santé" CNRS

BRAC DE LA PERRIERE M., « Données de santé, défi de sécurité et nécessité de réutilisation » DSIH, 15 février 2022

EL KALAM A., « Gestion des données médicales anonymisées : problèmes et solutions. » 2004, pp. Mons, Belgique, 9-11 octobre 2004

EON F., "Mise à disposition des données de santé", Expertises, 2017, page 428

GAMBARDELLA S., « Une lecture de la jurisprudence de la Cour européenne des droits de l'Homme relative aux données de santé. *Revue de droit sanitaire et social*, Sirey, Dalloz, 2016.

GIRARD M, POLTON D. « La nouvelle réglementation sur l'accès aux données de santé et sa mise en œuvre deux ans après la loi de modernisation de notre système de santé », *Journal du Droit de la Santé et de l'Assurance - Maladie (JDSAM)*, vol. 20, no. 3, 2018, pp. 25-29.

GRUSON D., « Le pilotage par les données : une révolution pour le droit et le management de la santé » RGDM, n 68, 2018, page 155

KERMARREC J-M., « Stop Covid, une mise en demeure de circonstance clôturée par la CNIL en 51 jours… » à propos de la décision n° MED-2020-015 du 15 juillet 2021, RDSS n°98, page 1165.

MENVIELLE L., « Effets de la fréquence d'utilisation des communautés virtuelles de patients sur la relation patients-médecins », Journal de gestion et d'économie médicales, vol. 34, no. 8, 2016

TRUCHET D., « Le droit des données de santé », Numéro spécial RGDM, 2004

4. *Dossiers et rapports :*

CNIL air2021 ; "Entre partage et protection : quelle éthique pour l'ouverture des données ? "

CLUSIF 2021 : "Le traitement des données de santé"

Rapport d'information du Sénat fait au nom de la délégation sénatoriale à la prospective sur les crises sanitaires et outils numériques : répondre avec efficacité pour retrouver nos libertés, Par Mmes Véronique GUILLOTIN, Christine LAVARDE et M. René-Paul SAVARY,

Conseil de l'Europe/Cour européenne des droits de l'homme : « Guide sur la jurisprudence de la Convention européenne des droits de l'homme, Protection des données » Première édition – 31 décembre 2020

Conseil d'État, Discours de Jean-Marc Sauvé, « La protection des droits fondamentaux à l'ère du numérique », 12 décembre 2017

5. *Textes officiels :*

Charte Européenne des Droits Fondamentaux de l'Union Européenne, 2000

Code civil 2022 annoté, 121ème édition, Dalloz

Code de déontologie médicale et décret n° 95-1000 du 6 septembre 1995 portant code de déontologie médicale

Code de la santé publique 2022 annoté, 36ème édition, Dalloz

Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personne - Strasbourg, 28.I.1981

Déclaration d'Helsinki de l'Association médicale mondiale ; Principes éthiques applicables aux recherches médicales sur des sujets humains. Adoptée par la 18e Assemblée générale, Helsinki, Juin 1964

Décret n° 2019-536 du 29 mai 2019 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés

Décret n° 2020-1690 du 25 décembre 2020 autorisant la création d'un traitement de données à caractère personnel relatif aux vaccinations contre la covid-19

Décret n° 2021-848 du 29 juin 2021 relatif au traitement de données à caractère personnel dénommé « système national des données de santé »

Directive 95/46/CE du Parlement européen et du Conseil, du 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

Directive (UE) 2016/680 du Parlement Européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données

Groupe de travail « Article 29» sur la protection des données, 0829/14/FR : Avis 05/2014 sur les Techniques d'anonymisation

Groupe de travail « Article 29 » : Lignes directrices sur le consentement au sens du règlement 2016/679, 17/FR WP259, Version du 10 avril 2018

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

Loi n° 88-1138 du 20 décembre 1988 relative à la protection des personnes qui se prêtent à des recherches biomédicales

Loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel

Loi n° 2004-806 du 9 août 2004 relative à la politique de santé publique

Loi n° 2012-300 du 5 mars 2012 relative aux recherches impliquant la personne humaine

Loi n°2004-810 du 13 aout 2014 relative à l'assurance maladie
Loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé
Loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles
Ministère chargé de la Santé, représenté par la Délégation à la stratégie des systèmes d'information de santé : « Explicitation du champ d'application du cadre juridique de l'hébergement de données de santé » 16 mai 2019
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

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

TABLE DES MATIÈRES

Les données de santé des patients sont sensibles et font l'objet d'une interdiction de traitement informatique, posée par la Loi Informatiques et Libertés, ainsi que par l'article 9 du RGPD. Néanmoins, au regard de leur intérêt pour la santé publique et pour l'avancé des innovations et recherches médicales, des exceptions à ce principe sont aménagées permettant aux professionnels de santé, aux agences sanitaires et à l'Etat de les utiliser. A l'heure où la pandémie de Covid a bouleversé les pratiques médicales, en renforçant notamment l'usage du numérique en santé, l'Europe adopte une position vigilante face aux utilisations des données de santé. Pour ce faire, les textes imposent que le traitement des dites-données soit fondé juridiquement et prévu par une des exceptions au principe d'interdiction du traitement des données de santé. Le consentement du patient est l'une d'entre elle, mais il est sollicité de manière marginale. L'intérêt public ou la prise en charge sanitaire permettent d'obtenir une autorisation d'utilisation moins contraignante des données médicales, ce qui conduit à s'interroger sur la pertinence du consentement comme exception à l'interdiction de traitement.

Un traitement conforme des données de santé nécessite également le respect d'un panel de droits, accordés au patient, se superposent à ses droits traditionnellement acquis lorsqu'il est à l'hôpital. Cela fait peser sur les hôpitaux, les professionnels de santé et les organismes de santé, un devoir d'information. Pour les médecins, il s'ajoute à l'obligation d'information aménagée par le Code de la santé publique et le Code de déontologie médicale. Enfin, l'étude du traitement des données de santé ne serait pas complète sans une attention portée au contrôle exercé par les juridictions et la CNIL, instance de régulation des données personnelles. Leur travail s'accroit au fil des atteintes portées aux données de santé, dont l'exploitation peut être malveillante du fait de la sensibilité des informations médicales qu'elles contiennent.

Mots clés : données de santé – RGPD – traitement – consentement – santé publique – numérisation de la santé

Patients' health data are sensitive and are the subject of a ban on computer processing, laid down by the French Data Protection Act and Article 9 of the GDPR. Nevertheless, in view of their interest for public health and for the advancement of medical innovations and research, exceptions to this principle are provided allowing health professionals, health agencies and the State to use them. At a time when the Covid pandemic has disrupted medical practices, notably by strengthening the use of digital in health, Europe is taking a vigilant position with regard to the uses of health data. In order to do this, the texts require that the processing of said data be legally based and provided for by one of the exceptions to the principle of prohibition of the processing of health data. Patient consent is one of them, but it is sought marginally. The public interest or health management allows a less restrictive use of medical data, which leads to questions about the relevance of consent as an exception to the prohibition of Article 9 of the GDPR.
A consistent treatment of health data also requires the respect of a panel of rights, granted to the patient, are superimposed on his traditionally acquired rights when he is in the hospital. This imposes an increased duty of information on hospitals, health professionals and health organizations. For physicians, it is in addition to the obligation to provide information set out in the Public Health Code and the Code of Medical Ethics. Finally, the study of health data processing would not be complete without attention to the control exercised by the courts and the CNIL, the regulatory body for personal data. Their work is increasing as health data are breached, the exploitation of which can be malicious due to the sensitivity of medical informations they contain.

Keywords: health data – GDPR – treatment – consent – public health – health digitization